


GistF.No. Z.18015/23/2017-eGov

In order to address the needs identified and delineated for regulation, data privacy and security etc. in Indian e-Health System, it was decided in this Ministry to set up a Nodal Body in the form of an Authority through an Act of Parliament. For drafting the Act, National Law School of India University, Bengaluru was mandated. The draft Act for setting up the Central Authority by name National Digital Health Authority of India has now been finalized (F/M').

2. It was also decided in this Ministry to put the draft Act on public domain for a period of one month seeking suggestions/comments from general public by 31.05.2017. Hon'ble MoS(AP), while taking review meeting with e-Health division on 15.05.2017 had directed that this deadline be met with.

3. This file is put up seeking approval of Hon'ble HFM for putting the Draft Act on Public Domain.

4. Hon'ble MoS(AP) may kindly approved the file to be sent to Hon'ble Minister of Health and Family Welfare.

  
(Dr. A. Madhavan)  
Sr. Consultant  
25-05-2017

# **NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA ACT**

**Draft 01.05.2017**

**Ministry of Health & Family Welfare,  
Government of India**

**INDEX**

<b>SL. NO.</b>	<b>PARTICULARS</b>	<b>PAGE NO.</b>
1	CHAPTER I – PRELIMINARY	2
2	CHAPTER II - DATA OWNERSHIP, SECURITY AND STANDARDIZATION	8
3	CHAPTER III - NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA	20
4	CHAPTER IV- HEALTH INFORMATION EXCHANGE	29
5	CHAPTER V- DIGITAL HEALTH CARE DATA BREACH AND CONSEQUENCES	42
6	CHAPTER VI- ADJUDICATING AUTHORITY AND APPELLATE AUTHORITY	48
7	CHAPTER VII- MISCELLANEOUS PROVISIONS	65

## NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA ACT, (INSERT YEAR)

---

*An Act to provide for establishment of National Digital Health Authority of India and Health Information Exchanges; and to provide for effective digital health care data privacy, confidentiality, security and standardization; and such other matters related and incidental thereto.*

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

### CHAPTER I PRELIMINARY

---

#### 1. SHORT TITLE, EXTENT

- (1) This Act may be called as National Digital Health Authority of India Act, (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

#### 2. COMMENCEMENT AND APPLICATION

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.



- (2) Save as otherwise expressly provided by the Central Government by Notification, this Act shall apply to all digital medical records, digital health records or digital personal/protected health data as the case may be.

### **3. ACT TO SUPERSEDE ANY OTHER LAW**

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health care data' hereunder.

### **4. DEFINITIONS**

- (1) In this Act, unless the context otherwise requires,
- (a) **'Anonymization'** means the process of permanently eliminating the identity of the owner and his/her digital health data, which may include removal of names or address or numbers or marks or telephone number or such government issued identification number or card etc.
  - (b) **'Breach'** means and includes the breach of digital health care data as per section 39 of this Act.

- (c) **'Consent'** means informed consent by the owner for collection or storage or dissemination of digital health care data already collected or to be collected and shall include subject to the circumstances envisaged under this Act, proxy consent on behalf of the owner.
- (d) **'De-identification'** means and includes the process of removing or obscuring any personally identifiable information from individual health-data in a manner that eliminates the risk of unintended disclosure of the identity of individuals and health information about them.
- (e) **'Digital Health Care Data'** is any data about the individual collected and/or recorded digitally in the course of provisioning of health services to the individual or otherwise, by the Health Service Provider or Health Information Exchange, and the said expression shall mean and specifically include the following:
  - (i) All data pertaining to the health status of the owner;

- (ii) All information collected about the individual during the process of registration to provide health services;
  - (iii) Information about payments or eligibility for healthcare with respect to the individual;
  - (iv) A number, symbol or such other particular assigned to an individual to uniquely identify the individual for health purposes;
  - (v) Information derived from the testing or examination of a body part or bodily substance, including biological samples;
  - (vi) Identification of person as provider of health care to the individual;
  - (vii) Any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.
- (f) **‘Entity’** means a person, or a partnership, or any other incorporated or

unincorporated association or body; or a trust or part of an entity.

- (g) **'Guardian'** means a parent or spouse or brother or sister or any relative or in some circumstances an attendant or person appointed by Court or such other person to be specified.
- (h) **'Health Informatics'** – the expression shall generically mean and include interdisciplinary study of the design, development, adoption, and application of information technology based innovations in healthcare services delivery, management, and planning.
- (i) **'Health Information Exchange'** means Health Information Exchange as recognized under this Act.
- (j) **'Health Service Provider'** is an entity registrable under sub-section (c) of Section 2 of Clinical Establishment (Registration & Regulation) Act, 2010, as a 'Clinical Establishment'; or any other equivalent law for the time being in force and such other entity or class of entities which Central Government shall declare by Notification.

- (k) **'Owner'** is an individual to whom the digital health care data belongs to, as per Section 5 of the Act.
- (l) **'Prescribed'** shall mean rules prescribed by the Central Government.
- (m) **'Privacy'** is a right of an individual as recognized by Indian Courts and specifically mean to suggest (to this statute) the right of an individual to control or influence what digital health care data related to him may be collected or stored or transmitted by whom, or how and when and to whom that digital health care data may be disclosed.
- (n) **'Security'** refers directly to protection, and specifically to the means used to protect the privacy of health information and support professionals in holding that information in confidence.
- (o) **'Specified'** shall mean as specified by National Digital Health Authority of India.
- (p) **'Transmission of Digital Health Care Data'** shall mean transmission of Digital health care data, for the purposes of this Act, and means to communicate the digital health care data or to release it to another.

## **CHAPTER II DATA OWNERSHIP, SECURITY AND STANDARDIZATION**

---

### **5. OWNERSHIP OF DIGITAL HEALTH CARE DATA**

- (1) The Digital health care data generated or collected or transmitted shall be owned by the individual to whom the digital health care data belongs to;
- (2) Health Service Provider or Health Information Exchange shall hold such digital health care data referred to in subsection (1) above in trust for the owner;
- (3) Notwithstanding anything stated above in this section, the medium of storage and transmission of digital health care data shall be owned by the Health Service Provider or Health Information Exchange as the case may be.

### **6. ENTITIES TO COLLECT DIGITAL HEALTH CARE DATA AS PER THE PROVISIONS OF THIS ACT**

- (1) Health Service Provider or Health Information Exchange shall collect or store or transmit either within India or abroad any digital health care data, strictly as per the provisions of this Act.
- (2) Further, entities other than the Health Service Provider or Health Information Exchange collecting or storing or transmitting either

within India or abroad, shall be notified by the Central Government for the purposes of this Act.

## **7. COLLECTION OF DIGITAL HEALTH CARE DATA**

- (1) Health Service Provider or Health Information Exchange, as the case may be, shall by express consent from the owner lawfully collect the required digital health care data as per the prescribed norms by the National Digital Health Authority of India, subsequent to, adequately informing the owner;
  - (a) The purpose of collection of such health data;
  - (b) The digital health care data to be collected;
  - (c) The entity or group or individual to whom the digital health care data shall be transmitted or disclosed;
  - (d) The entity or group or individual who shall have access to such collected digital health care data.
  - (e) The rights of the owner over the digital health care data as described in this Act.
- (2) Without prejudice to sub-section (1) above, the digital health care data can be collected by Health Service Provider or Health Information Exchange as the case may be, of an individual

who is incapacitated or incompetent to provide consent, by obtaining proxy consent from spouse or parent or legal guardian or attendant or such other person to be prescribed.

**Explanation 1:** For the removal of any ambiguity it is stated that, in case of proxy consent the person providing proxy at the time of contingency, shall have legal capacity to consent for the process of obtaining digital health care data of an individual.

**Explanation 2:** In case of temporary health scenarios the consent of the digital health care data owner may be taken once the person is back in to sensibility of legally consenting and exercising the legal rights.

- (3) National Digital Health Authority of India may prescribe suitable norms in this regard by Notification.

**8. STORING OF DIGITAL HEALTH CARE DATA**

- (1) Subject to the requirements and restrictions under this Act, digital health care data shall be stored, with Health Service Provider or Health Information Exchange, as the case may be, in accordance with the prescribed standards by the National Digital Health Authority of India in consultation with the Central Government.



- (2) Further the digital health care data collected and stored as per sub-section (1) above, with Health Service Provider or Health Information Exchange, shall be de-identified or anonymized, as the case may be, to ensure the right to privacy & confidentiality of the owner, by adopting such means or methods as may be prescribed.
- (3) Notwithstanding anything stated in this Act, or any other statute in force, all de-identified and anonymized digital health care data stored as per this Act, shall be deemed to be held by the concerned Health Service Provider or Health Information Exchange, as the case may be on behalf of National Digital Health Authority of India; and such digital health care data be used for such analysis or prediction of spread of diseases or prevalence of diseases or policy formation or such other purposes, without compromising the privacy or confidentiality of the owner.

Provided further that, the digital health care data shall vest with National Digital Health Authority of India, immediately after the death of the owner of the digital health care data.

- (4) The digital health care data vested with National Digital Health Authority as per sub-section (3) above, shall be stored or transmitted or used in such a manner as may be prescribed by the National Digital Health Authority of India in consultation with the Central Government.
- (5) The digital health care data vested with National Digital Health Authority of India as per sub-section (3) above shall not be transmitted or be used, if such transmission or use places the successor or decedents as the case may be, of deceased to plausible stigma.

Provided further that, National Digital Health Authority of India may specify norms by Notification in this regard.

#### **9. ACCESS TO DIGITAL HEALTH CARE DATA WITHIN HEALTH SERVICE PROVIDER**

- (1) The digital health care data collected or stored or received by Health Service Provider or Health Information Exchange as the case may be shall be accessed by only such professionals or otherwise, on need to know basis.

**Explanation:** for eliminating any ambiguity it is stated that, without prejudice to sub-section (1)

above, within Health Service Provider or Health Information Exchange as the case may be collecting digital health care data for the purposes of this Act, the concerned doctor or specialist or professional nursing staff or such other professional class of people to be prescribed, examining or performing such other related activities shall only have access to the digital health care data.

- (2) Notwithstanding anything stated in this Act, the immediate family member of an owner may have access to digital health care data during health emergencies;
- (3) Notwithstanding anything stated in this Act, in case of investigation into cognizable offences, digital health care data related information, may be accessed for the purposes of investigation by the investigating authority with the order of the Competent Court;
- (4) Health Service Provider or Health Information Exchange as the case may be, shall maintain the register in digital form to record the purposes and usage of digital health care data accessed within such Health Service Provider or Health Information Exchange, in the prescribed form by the National Digital Health Authority of India.

## **10. THE RIGHTS OF THE OWNER**

- (1) The owner shall have the right to deny collection of digital health care data at any time of such collection, subject to Public order and Public Health Emergency scenarios as notified by the Central Government.
- (2) The owner of the digital health care data shall have the right to know the data collected is relevant to the health service sought; and no excess data is collected.
- (3) The owner of the digital health care data shall have the right to know the entities who shall have access to and to whom the digital health care data shall be transmitted or disclosed.
- (4) The owner of the digital health care data shall have, subject to sub-section (1) to (3) above:
  - (a) The right to withdraw or seek for rectifying the digital health care data; or
  - (b) The right to convert the digital health care data into de-identified data; or
  - (c) The right to seek for erasing or rectification of the incorrect digital health care data stored, from the respective Health Service Provider or Health Information Exchange in the prescribed

form notified by the National Digital Health Authority.

## **11. THE DUTIES OF THE HEALTH SERVICE PROVIDER OR HEALTH INFORMATION EXCHANGE**

- (1) Except where this Act provides otherwise, the Health Service Provider or Health Information Exchange shall be bound to follow the mandate and standards prescribed under this Act in
  - (a) Collecting the digital health care data from an individual as prescribed under this Act;
  - (b) Storing the digital health care data securely by adopting prescribed standard norms;
  - (c) Allowing access to such collected data to only on 'need to know basis';
  - (d) Maintaining digital records of collected digital health care data in a prescribed manner, to access records for future retrieval;
  - (e) Not to transmit the data any further in contravention of this Act and regulate thereunder;
  - (f) Providing the digital health care data back to the owner on demand made in the prescribed format;

- (g) Providing proper notice immediately or within three working days to the owner whenever any digital health care data breach takes place;

**12. THE PROCEDURE FOR RETRIEVAL OR ANONYMIZATION OF DIGITAL HEALTH CARE DATA BY THE OWNER**

- (1) The owner of the digital health care data shall have an inalienable right to retrieve his digital health care data by making an application in a prescribed form to the Health Service Provider or Health Information Exchange as the case may be;
- (2) On such application under sub-section (1) by the owner for retrieval, the Health Service Provider or Health Information Exchange as the case maybe, shall provide such digital health care data requisitioned immediately or within the same date of such requisition.

**Provided** that, in case of emergency the requisitioned digital health care data may be provided immediately without any delay.

- (3) The owner of the digital health care data shall have the right to seek for erasing or rectifying the incorrect digital health care data stored in

any Health Service Provider or Health Information Exchange as the case may be.

Provided further that, the Health Service Provider or Health Information Exchange shall erase such digital health care data immediately or within three working days counted from the date of receipt of such application and the same shall be intimated to the owner.

### **13. TRANSMISSION OF DATA**

- (1) The digital health care data collected by Health Service Provider or Health Information Exchange as mentioned under this Act be transmitted with encryption to the designated Health Information Exchange or Health Information Exchanges.
- (2) Without prejudice to foregoing sub-section the digital health care data be transmitted securely and instantaneously after retaining a copy of the same for reasonable use by the Health Service Provider or Health Information Exchange as the case may be.

**Provided** that such transmitted data is de-identified at the Health Information Exchange. Further, for such secure and instantaneous

transmission of digital health care data National Digital Health Authority of India may prescribe such technical standards, keeping the privacy and confidentiality of the owner in mind, by notification.

- (3) The Health Service Provider shall have such digital health care data pertaining to an individual, transmitted to him, upon express consent from the owner.

**Provided** the National Digital Health Authority of India may prescribe standards and such other norms for this transmission of digital health care data between Health Information Exchange and Health Service Provider.

- (4) The Health Information Exchange shall maintain a Register in a prescribed format containing all details of the transmissions of the digital health care data between Health Information Exchange/s and Health Service Provider or between Health Information Exchanges.

#### **14. THE PROCEDURE OF TRANSMISSION OF DATA**

- (1) Without prejudice to any other provisions in this Act, the National Digital Health Authority of India shall prescribe the standards or norms for transmission of digital health care data.



- (2) The National Digital Health Authority of India shall prescribe standards or norms under sub-section (1) above for
- (a) Transmission of digital health care data between Health Service Provider to Health Information Exchange or Health Information Exchanges; or
  - (b) Transmission of digital health care data between Health Information Exchanges per se; or
  - (c) Transmission of digital health care data between Health Information Exchange or Health Information Exchanges and Health Service Provider.

## **15. STANDARDIZATION OF DIGITAL HEALTH CARE DATA**

- (1) Notwithstanding anything stated in this law or in any other law for the time being in force, the National Digital Health Authority of India shall prescribe standards in collecting, storing, transmitting the digital health care data and any other standards required for the said purposes under this Act;
- (2) Provided further that, the Health Service Provider or Health Information Exchange shall implement standards as prescribed by the National Digital Health Authority to:

- (a) Ensure the confidentiality, integrity, and availability of all the digital health care data created, transmitted, received, or maintained;
- (b) Protect against reasonably anticipated threats or hazards to the security of the health data;
- (c) Protect against uses or disclosures of the digital health care data that are not required or permitted under the prescribed standards;
- (d) Ensure their personnel to comply with their security policies and procedures.

### **CHAPTER III**

## **NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

### **16. NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

- (1) The Central Government shall establish the National Digital Health Authority of India by Notification, which may be referred to as NDHAI in its abbreviated form.
- (2) The National Digital Health Authority of India shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government, specifies a separate date in the same Notification.

## **17.COMPOSITION OF NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

- (1) National Digital Health Authority of India shall consist of the following members, to be appointed by Central Government by Notification, namely:
  - (a) A full time Chairman;
  - (b) Four full-time members to be appointed by the Central Government, in consultation with the Chairman;
  - (c) A member-secretary, among the four full-time members appointed as per sub-section (b) above;
- (2) Provided that, National Digital Health Authority of India shall co-opt such number of part-time members, not exceeding ten at any given point of time, who shall contribute specialized domain knowledge or need or expertise as the case may be.
- (3) Without prejudice to anything stated above, the Chairman and four full time members shall have the following qualifications:
  - (a) Be not less than forty years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge

and expertise of at least Ten years in any of the following areas,

- (i) Information Technology (IT); or
- (ii) Health Informatics; or
- (iii) Medicine; or
- (iv) Judiciary; or
- (v) Clinical care; or
- (vi) Public Health; or
- (vii) Health Service Delivery; or
- (viii) Health systems related research; or
- (ix) Related Academics; or
- (x) Law; or
- (xi) Public policy.

**Provided** that, to be appointed as Chairman, the person shall additionally have demonstrable qualities of leadership, institution building and cause of commitment.

- (c) Provided further that, a person shall be disqualified for appointment as per sub-section (1) above, if he –
  - (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (ii) Is an undercharged insolvent; or

- (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
- (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
- (v) Has such other disqualification as may be prescribed by the Central Government.

#### **18. TERM OF OFFICE OF CHAIRMAN & OTHER MEMBERS**

- (1) The Chairman and other members shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty years, whichever is earlier.
- (2) The Chairman and other Members, appointed as per sub-section (3) of section 17, are eligible for reappointment for another term or such other terms as the case may be; provided such reappointed Chairman or Member does not exceed sixty years of age.

- (3) The co-opted member shall hold office at the pleasure of the Authority, not exceeding two years from the date of appointment.

#### **19. SALARY, ALLOWANCE, BENEFITS AND SERVICE CONDITIONS ETC.,**

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairman and full-time members shall be such as may be prescribed.
- (2) Notwithstanding anything stated in sub-section (1) above, the salary, allowances and other conditions of service of the Chairman or of a member shall not be varied to his disadvantage after his appointment.
- (3) Co-opted additional members, appointed as per sub-section (2) of section 17 shall receive such allowances as may be prescribed.

#### **20. RESIGNATION, REMOVAL OF CHAIRMAN OR MEMBER**

- (1) The Chairman or full time member appointed under sub-section (1) of section 17
  - (a) May relinquish his office by submitting the resignation in writing to the Central Government; or
  - (b) May be removed from his office in accordance with the provisions of section 22.

- (2) The Co-opted member appointed as per sub-section (2) of section 17 may relinquish his office by submitting the resignation in writing to the Chairman;
- (3) The Chairman or any full-time member ceasing to hold office as per sub-section (1) above shall not accept any commercial employment, for a period of two years from the date of relinquishment, unless the Central Government exempts him from this disability.

## **21. RECONSTITUTION OF THE AUTHORITY**

Any vacancy caused to the office of the Chairman or any other member shall be filled up by the Central Government immediately or within a period of three months from the date on which such vacancy occurs.

## **22. REMOVAL IN CERTAIN CIRCUMSTANCES**

- (1) The Central Government may remove from office the Chairman or any full-time member, who –
  - (a) Has been adjudged as an insolvent; or
  - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (c) Has become physically or mentally incapable of acting; or
  - (d) Has acquired such financial or other interest as is likely to affect prejudicially

his functions as the Chairman or member;  
or

(e) Has so abused his position as to render his continuance in office prejudicial to the public interest.

(2) No such member or Chairman shall be removed from his office under clause (d) or clause (e) of sub-section (1) above, unless he has been given a reasonable opportunity of being heard in the matter.

### **23. OFFICERS AND OTHER EMPLOYEES OF THE AUTHORITY**

(1) The National Digital Health Authority of India in consultation with Central Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.

(2) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the Authority appointed under sub-section (1) shall be such as may be prescribed.

### **24. POWERS AND FUNCTIONS OF NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

(1) The National Digital Health Authority of India to ensure confidentiality and privacy of digital



health care data shall have the following powers and functions

- (a) Grant of recognition to such Health Information Exchanges, which fulfill the criteria prescribed.
- (b) Formulate standards for the collection or storage or transmission of the digital health care data;
- (c) Lay down the operational guidelines or protocols for the collection or storage or transmission of the digital health care data or such other said purposes under this Act;
- (d) Establish the procedure for the collection or storage or transmission of the digital health care data or such other said purposes under this Act;
- (e) Notify and mandate the Health Service Providers or Health Information Exchanges as the case may be, in case of failure to comply with the provisions of this Act;
- (f) Conduct investigations to ensure the compliance with any of the provisions of this Act;

- (g) To act as focal agency in processing the transmission of digital health care data to abroad;
- (h) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
- (i) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.

## **25. OVERSIGHT, INSPECTION, ISSUANCE OF DIRECTIONS ETC.**

- (1) To carry out all or any of the powers and functions enumerated in Section 24, the National Digital Health Authority of India shall have the right to inspect all such records; or access the premises, including virtual premises of the Health Information Exchange and Health Service Provider at any time.

**Provided** that National Digital Health Authority of India while accessing such records or accessing either the physical or virtual premises of Health Information Exchanges and

Health Service Providers, shall bear in mind that no or least possible hindrance is caused to the normal working of the Health Information Exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Digital Health Authority of India to generally discharge its functions under this Act, shall direct a Health Information Exchange and Health Service Provider, or class of Health Information Exchanges, or all Health Information Exchanges as the case may be, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the National Digital Health Authority of India are binding upon the Health Information Exchange or Health Information Exchanges and health Service Providers as the case may be.

## **Chapter IV**

### **HEALTH INFORMATION EXCHANGE**

---

#### **26. RECOGNITION OF HEALTH INFORMATION EXCHANGE**

- (1) No entity shall operate as Health Information Exchange in India, unless duly recognized by the National Digital Authority of India.

- (2) Any Health Information Exchange, which is desirous of operating as such for the purposes of this Act, may make an application in the prescribed manner to the National Digital Health Authority of India.
- (3) Every application under sub-section (2) shall contain such particulars as may be prescribed.

## **27. GRANT OF RECOGNITION**

- (1) If the National Digital Health Authority of India is satisfied, after making such an inquiry as may be necessary in this behalf and after obtaining such further information, if any, as it may require; but satisfying itself that if granted recognition privacy and confidentiality of the digital health care data will sufficiently be protected, may grant recognition to such Health Information Exchange.
- (2) Without prejudice to sub-section (1) above, National Digital Health Authority of India may grant recognition subject to such condition or conditions as it may desire.
- (3) Every grant of recognition to the Health Information Exchange under this Section shall be published in the Gazette of India; and such recognition shall have effect as from the date of its publication in the Gazette of India.

- (4) No application for grant of recognition shall be refused except after giving an opportunity to the applicant concerned to be heard in the matter; and the reasons for such refusal shall be communicated in writing.
- (5) Any person aggrieved by either grant of recognition or refusal of recognition as per subsection (4) above, may prefer an appeal to the Central Government, within thirty days.

**Provided** the Central Government may relax the limitation period of thirty days, if there is justifiable cause for the aggrieved person for not filing his grievance within thirty days, by an order in writing by assigning reason for such relaxation.

## **28. WITHDRAWAL OF RECOGNITION**

If the National Digital Health Authority of India is of the opinion that the recognition granted to a Health Information Exchange under the provisions of this Act shall, in the interest of digital health care data collected or stored or transmitted or in the public interest, be withdrawn – may serve a written notice of 30 days that, the National Digital Health Authority of India is considering the withdrawal of the recognition for the reasons stated in the notice, and after giving an opportunity to the concerned Health Information

Exchange to be heard in the matter, may withdraw by Notification in the Official Gazette, the recognition granted to the Health Information Exchange.

## **29. THE MANAGEMENT OF HEALTH INFORMATION EXCHANGES**

- (1) All Health Information Exchanges, recognized under Section 26, shall conduct and carry out its affairs strictly as per the norms and standards prescribed by the National Digital Health Authority of India from time to time.
- (2) Without prejudice to any other stipulations of this Act, the Health Information Exchange recognized under section 26 shall only employ such skilled personnel for management of its affairs as may be specified by the National Digital Health Authority of India.

## **30. THE CHIEF HEALTH INFORMATION EXECUTIVE (CHIE)**

- (1) The Health Information Exchange recognized under this Act, shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the National Digital Health Authority of India.
- (2) The Chief Health Information Executive as appointed under sub-section (1) above, shall be the Chief Executive Officer and also the data

controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs.

### **31. FUNCTIONS OF THE CHIEF HEALTH INFORMATION EXECUTIVE**

Being the Chief Executive Officer of the Health Information Exchange, he shall –

- (1) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
- (2) Access and transmit and process the digital health care data transmitted by the Health Service Providers to further transmit the digital health care data, whenever required, in accordance with norms prescribed by the National Digital Health Authority of India.
- (3) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
- (4) Notify the data breach to the owner and such other concerned.
- (5) Store the digital health care data in de-identified or anonymized mode as the case may in all situations.

### **32. POWERS AND RESPONSIBILITIES OF THE CHIEF HEALTH INFORMATION EXECUTIVE**

- (1) The Chief Health Information Executive shall be deemed to be endowed with all such powers to carry out efficiently and effectively all the functions indicated in Section 31 of the Act.
- (2) The Chief Health Information Executive shall be directly held responsible to ensure that all the indicated functions in Section 31 are carried out effectively and efficiently.

### **33. DE-IDENTIFIED DIGITAL HEALTH CARE DATA KEY AND ANONYMIZED DIGITAL HEALTH CARE DATA**

- (1) The Chief Health Information Executive of the Health Information Exchange shall hold the key to link the de-identified data to the individual to whom the digital health care data belongs.
- (2) The key referred to in sub-section (1) shall be held securely by the Chief Health Information Executive, and establish the link while transmitting the digital health care data securely to other Health Information Exchange or Health Service Provider as the case may be.
- (3) The Chief Health Information Executive shall be the officer responsible to permanently destroy the link or key as the case may be, which shall establish the digital health care data's link with its owner, immediately after the receipt of information of owner's death by him.



**Provided** that the Central or State Government shall have access to both de-identified and anonymized digital health care data (without the identity key) from Health Information Exchange or Health Information Exchanges for the formulation of policy purposes.

#### **34. PERIODICAL REPORTS, DIRECT INQUIRIES ETC.**

- (1) Every recognized Health Information Exchange shall furnish to National Digital Health Authority of India such periodical returns relating to its affairs as may be prescribed.
- (2) Every recognized Health Information Exchange shall maintain and preserve for such periods as may be prescribed, the digital health care data and such other books of accounts; and other documents as the National Digital Health Authority of India may prescribe, and such digital health care data or books of accounts or such other documents shall be subject to inspection at all reasonable times by the National Digital Health Authority of India.
- (3) Without prejudice to anything stated in subsection (1) and (2) above, the National Digital Health Authority of India, if it is satisfied that it is in the interest of better implementation of this Act or in the public interest so to do, may by order in writing –

- (a) Call upon the Health Information Exchange or Health Information Exchanges thereof to furnish in writing such information or explanation relating to the affairs of the Health Information Exchange concerned as the National Digital Health Authority of India may require; or
  - (b) Appoint one or more of its Member or Members or person or persons to make an inquiry in the prescribed manner in relation to the affairs of the Health Information Exchange or Health Information Exchanges; and submit a report of the result of such inquiry to National Digital Health Authority of India, within such time as may be specified in the order.
  - (c) To have an inquiry conducted independently by the concerned Health Information Exchange or Health Information Exchanges, and submit the report to National Digital Health Authority of India, for further action or otherwise.
- (4) Where an inquiry in relation to the affairs of a recognized Health Information Exchange

regarding its affairs has been undertaken under sub-section (3) above –

- (a) Every director, manager, secretary or other officer of such Health Information Exchange;
- (b) Every member of such Health Information Exchange;
- (c) If the member of the Health Information Exchange is a firm; every partner, manager, secretary or other officer of the firm; and
- (d) Every other person or body of persons who has had dealings in the course of business with any of the persons mentioned in clauses (a), (b) and (c), whether directly or indirectly –

Shall be bound to produce before the authority making the inquiry all such books of account, and other documents in his custody or power relating to, or having a bearing on the subject-matter of such inquiry and also to furnish the authorities within such time as may be specified with any such statement or information relating thereto as may be required of him.

### **35. ANNUAL REPORTS TO BE FURNISHED TO NATIONAL DIGITAL HEALTH AUTHORITY BY HEALTH INFORMATION EXCHANGE**

Every recognized Health Information Exchange shall furnish to the National Digital Health Authority of India a copy of the annual report, and such annual report shall contain such particulars as may be specified.

### **36. POWER TO ISSUE DIRECTIONS**

- (1) Either generally or after an inquiry as indicated in this Act, the National Digital Health Authority of India, is satisfied that it is necessary in the interest of better implementation of this Act, or accomplish the objectives of this Act or in the public interest, may issue such directions to the Health Information Exchange or class of Health Information Exchanges as the case may be.
- (2) Without prejudice to anything stated in subsection (1) above, the power to issue directions by National Digital Health Authority of India, shall generally encompass the following –
  - (a) In the interest of owners of digital health care data;
  - (b) To prevent the affairs of Health Information Exchange or Health Information Exchanges, being conducted

in a manner detrimental to the overall public interest or the objectives of this Act;

- (c) To secure the proper management of storage and dissemination of digital health care data within the territory of India or abroad;

### **37. POWER TO SUSPEND THE BUSINESS OF RECOGNIZED HEALTH INFORMATION EXCHANGE**

- (1) If in the opinion of the National Digital Health Authority of India, an emergency has arisen and for the purpose of meeting the emergency the National Digital Health Authority of India considers it expedient so to do, it may, by notification in the Official Gazette, for the reasons to be set out therein, direct a recognized Health Information Exchange to suspend such of its business for such period not exceeding thirty days and subject to such conditions as may be specified in the Notification; and if in the opinion of the National Digital Health Authority of India, in the public interest that the period of suspension should be extended, may by Notification, extend the said period from time to time.

- (2) Without prejudice to sub-section (1) above, where the period of suspension is to be extended beyond the first period of thirty days, no Notification extending the period of suspension shall be issued unless the Central Government is consulted.

**38. POWER OF THE NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA TO SUPERSEDE THE GOVERNING BODY OF A RECOGNIZED HEALTH INFORMATION EXCHANGE**

- (1) Without prejudice to any other powers vested in the National Digital Health Authority of India under this Act, where the National Digital Health Authority of India is of the opinion that the governing body, by whatever name called, of any Health Information Exchange, should be superseded, then notwithstanding anything contained in any other law for the time being in force, the National Digital Health Authority of India, may supersede the governing body of the Health Information Exchange.
- (2) No superseding as envisaged under sub-section (1) above can take place, unless a written notice that, the National Digital Health Authority of India is considering the supersession of the governing body for the reasons specified in the notice and after giving an opportunity to the

governing body to be heard in the matter, and by notification in the Official Gazette, declare the governing body of such Health Information Exchange to be superseded, and appoint any person or persons to exercise and perform all the powers and duties of the governing body, and where more persons than one are appointed, may appoint one of such persons to be the Chairman.

- (3) Immediately on the publication of a notification in the Official Gazette under sub-section (2) above, the following consequences shall ensue –
- (a) The members of the governing body which has been superseded shall as from the date of notification of supersession, cease to hold office as such members;
  - (b) The person or persons appointed under sub-section (1) may exercise and perform all the powers, and duties of the governing body which has been superseded;
  - (c) All such property of the recognized Health Information Exchange as the person or persons appointed under sub-section (2) may, by order in writing, specify in this behalf as being necessary for the purpose of enabling him or them to carry on the

business of the Health Information Exchange, shall vest in such persons.

- (4) The National Digital Health Authority of India may at time before the determination of the period of office of any person or persons appointed under this section call upon the recognized Health Information Exchange to re-constitute the governing body in accordance with its rules and on such re-constitution all the property of the recognized Health Information Exchange which has vested in, or was in the possession of the person or persons appointed under sub-section (2), shall revert or vest as the case may be, in the governing body so re-constituted.

**Provided** that until a governing body is so re-constituted, the person or persons appointed under sub-section (2), shall continue to exercise and perform their powers and duties.

## **CHAPTER V**

### **DIGITAL HEALTH CARE DATA BREACH AND CONSEQUENCES**

---

#### **39. THE BREACH OF DIGITAL HEALTH CARE DATA**

- (1) The digital health care data under this Act is said to be breached, if,



- (a) The Health Service Provider and the Health Information Exchanges does any act which is in contravention of this Act; or
- (b) If the digital health care data stored or transmitted by any Health Information Exchange is not anonymized or De-identified as per the norms of this Act; or
- (c) Any person or entity(s) inadvertently does any act which is in contravention with this Act; or
- (d) Any person or entity(s) does anything which is in contravention with the exclusive right conferred upon the owner of the digital health care data; or
- (e) Any person or entity(s) un-authorizingly procures, stores or transmits the digital health care data; or
- (f) Any person or entity(s) un-authorizingly use the digital health care data for the purposes other than mentioned under this Act; or
- (g) Any person or entity(s) un-authorizingly uses the digital health care data for the Commercial Purposes/ Commercial gain; or

- (h) Any person or entity(s) causes any damage, destroys or deletes or affects it injuriously by any means or tampers any digital health care data existing in any digital form.
- (2) For the purposes of this Act, the Serious Digital health care data Breach shall be, if,
  - (a) The digital health care data breach of similar nature pertaining to the same individual for the second or repeated times; or
  - (b) Potential number of individuals are affected; or
  - (c) Involving serious digital health care data or other information of sensitive nature; or
  - (d) Whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference; or
  - (e) Vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted; or
  - (f) It involves deliberate or reckless conduct.

#### **40. PENALTIES**

- (1) Any person or entity or entities who contravene the provisions of sub-section (1) of section 39 shall be punished with simple imprisonment for

a term which shall extend up to two years and fine which shall be not less than one lakh rupees; or both.

- (2) Any person or entity or entities who contravene the provisions of sub-section (2) of Section 39 shall be punished with simple imprisonment which shall extend from two years and up to four years; and fine which shall not be less than five lakh of rupees.
- (3) Provided that, without prejudice to anything stated elsewhere, any fine imposed as part of sub-section (2) of this section may be provided to the individual by the Court, as it deems fit as compensation.

#### **41. PENALTY FOR FAILURE TO FURNISH INFORMATION, RETURN etc.,**

Any person or Health Information Exchange, which is required under this Act or any rules made thereunder to furnish any information or document or books or returns or reports etc., to National Digital Health Authority of India or such other designated Authority, by Central Government, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues;

#### **42. COGNIZANCE OF OFFENCES BY COURT**

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations or bye-laws made thereunder, save on complaint made by the Central Government or State Government or the National Digital Health Authority of India or such designated authority by the Central Government.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under this Act.

#### **43. OFFENCES BY COMPANIES**

- (1) Where an offence under this Act has been committed by a company or such other incorporated body, every person who, at the time when the offence was committed, was in charge of, and/or was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence, and shall be liable to be proceeded against and punished accordingly.

**Provided** that nothing contained in this subsection shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he exercised all due

diligence to prevent the commission of such offence.

- (2) Notwithstanding anything contained in sub-section (1) above, where an offence under this Act has been committed by a Company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any gross negligence on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.
- (3) **Explanation** – For the purpose of this Section –
- (a) **“Company”** shall mean anybody corporate and includes a firm or other association of individuals; and
  - (b) **“Director”** in relation to
    - (i) a firm, means a partner in the firm;
    - (ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;
- (4) The provisions of this section shall be in addition to, and not in derogation of other provisions of this Act.

## **CHAPTER VI**

### **ADJUDICATING AUTHORITY AND APPELLATE AUTHORITY**

---

#### **44. PERSON COMPLAINING TO ADJUDICATING AUTHORITY**

- (1) For any data breach an aggrieved person or owner may complain to the Adjudicatory Authority in writing as may be prescribed by Central Government, and seek reasonable monetary compensation (damages) for the digital health care data breach and consequence thereof.
- (2) No such complaint shall be made after two years from the date of, such person or owner coming to know about the digital health care data breach.
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification.
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time.

#### **45. ADJUDICATING AUTHORITIES, COMPOSITION, POWERS ETC.**

- (1) The Central Government shall by Notification, appoint an Adjudicating Authority or such number of Adjudicating Authorities, depending upon the local requirements, to exercise jurisdiction, powers and authority conferred by or under this Act.
- (2) An Adjudicating Authority shall consist of a Chairperson and two other members, provided that at least one of such person shall be from the field of law.
- (3) A person shall, however, not be qualified for appointment as Members of an Adjudicating Authority –
  - (a) In the field of law, unless he
    - (i) Is qualified for appointment as District Judge; or
    - (ii) Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
  - (b) In the field of medicine, information (health) science or administration unless he possesses such qualifications as may be prescribed by the Central Government.

- (4) The Central Government shall appoint a Member to be the Chairperson of the Adjudicating Authority.
- (5) Subject to the provisions of this Act,
  - (a) The jurisdiction of the Adjudicating Authority may be exercised by the Benches thereof;
  - (b) A Bench may be constituted by the Chairperson of the Adjudicating Authority may be exercised by Benches thereof;
  - (c) A Bench may be constituted by the Chairperson of the Adjudicating Authority with one or two Members as the Chairperson of the Adjudicating Authority may deem fit;
  - (d) The Benches of the Adjudicating Authority shall ordinarily sit at the State Capitals; and such other places as the Central Government may, in consultation with the Chairperson by notification, specify;
  - (e) The Central Government shall, by notification, specify the areas in relation to which each Bench of the Adjudicating Authority may exercise jurisdiction.
- (6) Notwithstanding anything contained in subsection (5), the Chairperson may transfer a Member from one Bench to another Bench.



- (7) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member that the case or matter is of such a nature that it ought to be heard by a Bench consisting of two Members, the case or matter may be transferred by the Chairperson or, as the case may be, referred to him for transfer, to such Bench as the Chairperson may deem fit.
- (8) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.

**Provided** that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.

- (9) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed by the Central Government.

**Provided** that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.

- (10) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government shall appoint another

person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.

- (11) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government, resign his office:

**Provided** that, the Chairperson or any other Member shall, unless he is permitted by the Central Government or relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (12) The Chairperson or any other Members shall not be removed from his office except by an order made by the Central Government after giving necessary opportunity of hearing.
- (13) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in

accordance with the provisions of this act to fill such vacancy, enters upon his office.

- (14) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (15) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

#### **46. STAFF OF THE ADJUDICATING AUTHORITY**

- (1) The Central Government shall provide each Adjudicating Authority with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees

of the Adjudicating Authority shall be such as may be prescribed by the Central Government.

#### **47. POWER REGARDING SUMMONS, PRODUCTION OF DOCUMENTS AND EVIDENCE**

(1) The Adjudicating Authority shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely

- (a) Discovery and inspection;
- (b) Enforcing the attendance of any person, including any officer of a Health Service Provider or a Health Information Exchange and examining him on oath;
- (c) Compelling the production of records;
- (d) Receiving evidence on affidavits;
- (e) Issuing commissions for examination of witnesses and documents; and
- (f) Any other matter which may be prescribed by the Central Government.

(2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or

make statements, and produce such documents as may be required.

- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

#### **48. ESTABLISHMENT OF APPELLATE TRIBUNAL**

The Central Government shall, by Notification, establish an Appellate Tribunal to hear appeals against the orders of the Adjudicating authority and authorities under this Act.

#### **49. APPEALS TO APPELLATE TRIBUNAL**

- (1) Save as otherwise provided in sub-section (2) below, any person aggrieved by an order made by the Adjudicating Authority under this Act, may prefer an appeal to the Appellate Tribunal.
- (2) Every appeal preferred under sub-section (1) above shall be filed within a period of forty-five days from the date on which a copy of the order made by the Adjudicating Authority is received and it shall be in such form and be accompanied by such fee as may be prescribed by the Central Government.

**Provided** that the Appellate Tribunal may after giving an opportunity of being heard entertain an appeal after the expiry of the said period of

forty-five days, if it is satisfied that there was sufficient cause for not filing it within that period.

- (3) On receipt of an appeal under sub-section (1) above, the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming or modifying or setting aside the order appealed against.
- (4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Adjudicating Authority.
- (5) The appeal filed before the Appellate Tribunal under sub-section (1) or sub-section (2) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within three months from the date of filing of the appeal.

**50.COMPOSITION ETC., OF THE APPELLATE TRIBUNAL**

- (1) The Appellate Tribunal shall consist of a Chairperson and two other Members.
- (2) Subject to the provisions of this Act.
  - (a) The jurisdiction of the Appellate Tribunal may be exercised by the Benches thereof;

- (b) A Bench may be constituted by the Chairperson with one or two Members as the Chairperson may deem fit;
  - (c) The Benches of the Appellate Tribunal shall ordinarily sit at New Delhi and such other places as the Central Government may, in consultation with the Chairperson, by Notification, specify.
  - (d) The Central Government shall, by Notification, specify the areas in relation to which each Bench of the Appellate Tribunal may exercise jurisdiction.
- (3) Notwithstanding anything contained in subsection (2), the Chairperson may transfer a Member from one Bench to another Bench.
- (4) If at any stage of hearing of any case or matter it appears to the Chairperson or a Member that the case or matter is of such a nature that it ought to be heard by a Bench consisting of two Members, the case or matter may be transferred by the Chairperson or, as the case may be referred to him for transfer, to such Bench as the Chairperson may deem fit.

## **51. QUALIFICATIONS FOR APPOINTMENT**

- (1) A person shall not be qualified for appointment as Chairperson unless he is or has been Judge of Supreme Court or of a High Court or is qualified to be a Judge of the High Court.
- (2) A person shall not be qualified for appointment as a Member unless he
  - (a) Has been a Member of the Indian Legal Service and has held a post in Grade I of that Service for at least three years; or
  - (b) Has been rendered at least ten years of service in Central Medical Services; or
  - (c) Such other relevant qualification to be prescribed by the Central Government.
- (3) No sitting Judge of the Supreme Court or of a High Court shall be appointed under this section except after consultation with the Chief Justice of India.
- (4) The Chairperson or a Member holding a post as such in any other Tribunal, established under any law for the time being in force, in addition to his being the Chairperson or a Member of that Tribunal, may be appointed as the Chairperson or a Member, as the case may be, of the Appellate Tribunal under this Act.



## 52. TERM OF OFFICE

The Chairperson and every other Member shall hold office as such for a term of five years from the date on which he enters upon his office.

**Provided** that no Chairperson or other Member shall hold office as such after he has attained

- (a) In case of the Chairperson, the age of sixty-eight years;
- (b) In the case of any other member, the age of sixty-five years.

## 53. CONDITIONS OF SERVICE

The salary and allowances payable to and the other terms and conditions of service (including tenure of office) of the Chairperson and other Members shall be such as may be prescribed.

**Provided** that, neither the salary and allowance nor the other terms and conditions of service of the Chairperson or any other Members shall be varied to his disadvantage after appointment.

## 54. VACANCIES

If, for reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government shall appoint another person in accordance with the provisions of this act to fill the vacancy and the

proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.

## **55. RESIGNATION AND REMOVAL**

- (1) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government, resign from his office;

**Provided** that the Chairperson or any other Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whoever is the earliest.

- (2) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government on the ground of proved misbehavior or incapacity, after an inquiry made by a person appointed by the President in which such Chairperson or any other Member concerned had been informed of the charges against him and given a reasonable opportunity of being heard in respect of those charges.

## **56. MEMBER TO ACT AS CHAIRPERSON IN CERTAIN CIRCUMSTANCES**

- (1) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior most Member shall act as the Chairperson until the date on which the new Chairperson, appointed in accordance with the provisions of this Act to fill such vacancy, enters upon his office.
- (2) When the Chairperson is unable to discharge his functions owing to absence, illness or any other cause, the senior most Member shall discharge the functions of the Chairperson until the date on which the Chairperson resumes his duties.

## **57. STAFF OF THE APPELLATE TRIBUNAL**

- (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may think fit.
- (2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of the Chairperson
- (3) The salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal shall be such as may be prescribed by the Central Government.

## **58. PROCEDURE AND POWERS OF APPELLATE TRIBUNAL**

- (1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.
- (2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint.
- (3) An order made by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court and, for this purpose the Appellate Tribunal shall have all the powers of the Civil Court.
- (4) Notwithstanding anything contained in subsection (3) above, the Appellate Tribunal may transmit any order made by it to the Civil Court having local jurisdiction and such Civil Court shall execute the order as if it were a decree made by that court.
- (5) All the proceedings before the Appellate Tribunal shall be deemed to be judicial

proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 (45 of 1860) and the Appellate Tribunal shall be deemed to be a Civil Court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

#### **59. Distribution of business among benches**

Where any Benches are constituted, the Chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the Benches and also provide for the matters which may be dealt with by each Bench.

#### **60. POWER OF THE CHAIRMAN TO TRANSFER CASES**

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may desire to be heard, or on his own motion without such notice, the Chairperson may transfer any case pending before one Bench, for disposal, to any other Bench.

#### **61. DECISION TO BE BY MAJORITY**

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson who shall either hear the point or points himself or refer the case for hearing on such point or points by third Member of the Appellate

Tribunal and such point or points shall be decided according to the opinion of the majority of the Members of the Appellate Tribunal who have heard the case, including those who first heard it.

## **62. MEMBERS ETC., TO BE PUBLIC SERVANTS**

The Chairperson, Members and other officers and employees of the Appellate Tribunal, the Adjudicating Authority and the officers subordinate to it shall be deemed to be public servants within the meaning of Section 21 of the Indian Penal Code, 1860 (45 of 1860).

## **63. CIVIL COURT NOT TO HAVE JURISDICTION**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Authority or the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

## **64. APPEAL TO HIGH COURT**

- (1) Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of law or fact arising out of such order.

- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

## **CHAPTER VII**

### **MISCELLANEOUS PROVISIONS**

---

#### **65. POWER OF THE CENTRAL GOVERNMENT TO MAKE RULES**

The Central Government may, by notification, make rules for the purposes of carrying out the provisions of this Act.

#### **66. REMOVAL OF DIFFICULTY BY THE GOVERNMENT**

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of

this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.

- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

#### **67. DIGITAL HEALTH CARE DATA TO BE USED FOR RESEARCH, ACADEMIC AND SUCH OTHER RELATED PURPOSES**

- (1) The Health Service Providers or Health Information Exchanges are compelled under this Act to maintain the anonymity of digital health care data to be transferred for the



research, academic and such other related purposes.

Such digital health care data transferred for research, academic and such other related purposes shall be used anonymously as prescribed by NDHAI.

## **Background Note**

**on**

## **Health Data Privacy & Security in India**

**Ministry of Health & Family Welfare  
Government of India**

## Introduction

- 1.1. Patient confidentiality and the protection of privacy is an essential requirement in health care. Patients must feel at ease sharing private & health information and medical history while availing healthcare services. Since healthcare is an information intensive and sensitive industry, healthcare personnel must take adequate measures while dealing with health/clinical information.
- 1.2. Possible privacy violations in the healthcare sector could include: disclosure of personal health information to third parties without consent, inadequate notification to a patient of a data breach, unlimited or unnecessary collection of personal health data, collection of personal health data that is not accurate or relevant, the purpose of collecting data is not specified, refusal to provide medical records upon request by client, provision of personal health data to public health, research & commercial uses without de-identification of data and improper security standards, storage and disposal.
- 1.3. There are a number of Health IT Systems currently implemented which collect health/clinical data of patients/citizens on a large scale. As a result huge health/clinical data repositories are being created. This requires adequate rules & regulations and institutional mechanism to address privacy & security related challenges/concerns.
- 1.4. This note has been drafted primarily for the purpose of outlining (a) key features pertaining to data privacy & security under various regulations in India specific to health domain & also in general like IT Act, 2000, (b) health data privacy & security regulations in other select countries, and (c) need for an appropriate framework/mechanism for addressing health data privacy & security in India. This paper provides an understanding of the current situation and spells out the need for addressing data privacy & security in health sector in India.

## Background / Indian experience

- 2.1. In India there are different legislations specific to particular health conditions/circumstances including mental/ physical illness, disability, communicable diseases etc. Key legislations/regulations in Health domain and their salient features pertaining to privacy/confidentiality are briefed subsequently. These include:
  - Medical Council of India's Code of Ethics Regulations, 2002
  - Epidemic Diseases Act, 1897
  - Mental Health Act, 1987
  - The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995

- Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994
  - Medical Termination of Pregnancy Act, 1971
  - Insurance Regulatory and Development Authority (Third Party Administrators) Health Services Regulations, 2001
  - Ethical Guidelines for Biomedical Research on Human Subjects
- 2.2. The Information Technology Act, 2000 (IT Act) provides legal recognition to any transaction, which is done by electronic way or use of Internet. The issue of data protection has been addressed in Information Technology Amendment Act, 2008. It protects private information that is obtained by agencies by virtue of powers conferred under the Act. Its salient features pertaining to privacy/confidentiality are briefed subsequently.
- 2.3. It has been observed that the existing legislations in health domain cover some aspects of privacy & security specific only to the mandated /limited scope. The IT Act, providing legal recognition to any transaction done by electronic way or use of Internet, covers issue of personal data protection, collected for specific purpose of electronic transaction. The key aspects which have been observed lacking under the existing legislations generally, include consent, collection & purpose limitation, access & correction, penalty/offenses/liability & remedy, security etc.
- 2.4. The need for a statute specifically covering data privacy & security aspects in a comprehensive manner in Health sector has been brought forward by the stakeholders at various forums in the past. Such need emerges more imperative in the context of promotion & adoption of eHealth on a large scale through establishment of pan-India Integrated Health Information System and EHR System including setting up of Health Information Exchanges under Digital India Programme.
- 2.5. In 2013, Ministry of Health & Family Welfare (MoHFW) formulated and notified the EHR Standards for India in consultation with various health care stakeholders, to take a step towards addressing the existing challenges of lack of standards and inter-operability amongst health information systems. The Notification of Standards also encompasses aspects related data ownership of EHR and accordingly the Ethical, Legal, Social Issues (ELSI) guidelines for Electronic Health Record (EHR) are recommended. The document on the notified EHR Standards for India is available at <http://www.mohfw.nic.in/showfile.php?lid=1672>.
- 2.6. Apropos the above, the Ministry has now constituted 'Legal Sub-group' under EMR/EHR Standards Committee specifically mandated to envisage mechanism/guidelines addressing privacy & security of patient health data/records, while at the same time ensuring accessibility to health records for academia, health care providers/centres/

hospitals etc. Legal Sub-group comprises members from different stakeholder groups including private health sector. The Legal sub-group has so far met on two occasions to deliberate on the subject.

- 2.7. After detailed deliberations the Legal Sub-group has decided to address health data privacy & security through a specific Act. It has been decided that the Act should also encompass setting up of Health Information Exchanges, to promote & facilitate exchange of patients' health records amongst different health care providers. A broad Table of Content (ToC) endorsed by the Legal Sub-group for the proposed Act is provided at Annexure I.
- 2.8. MoHFW has also proposed to set-up National eHealth Authority (NeHA) as a statutory body for promotion/adoption of eHealth standards, to regulate storage and exchange of Electronic Health Records. Concept Note on establishment of NeHA has been in public domain for inviting suggestions / feedback. A copy of the Concept Note is provided at Annexure II.

Table 2.1 : Legislations/ Regulations in India

Name	Brief features
Medical Council of India's Code of Ethics Regulations, 2002	<p>The Medical Council of India (MCI) Code of Ethics Regulations sets the professional standards for medical practice.</p> <p>It covers regulations for :</p> <ul style="list-style-type: none"> <li>- Patient Confidentiality</li> <li>- Data Access and Retention</li> <li>- Written Consent before performing an operation</li> <li>- Research : Publication of photographs or case studies without consent by patients is prohibited. If the identity of the patient cannot be discerned then consent is not needed. However, the method of consent, whether verbal or written, is not stated.</li> </ul>
Epidemic Diseases Act, 1897	<p>Under the Epidemic Diseases Act, if any part of the state is "visited by, or threatened with, an outbreak of any dangerous epidemic disease", the state government can enforce certain measures and prescribe regulations to prevent the outbreak or spread of a disease.</p> <p>Measures that impact privacy include:</p> <ul style="list-style-type: none"> <li>- Power to inspect : the State Government can undertake "inspection of persons travelling by railway or otherwise"</li> </ul>
Mental Health	The Mental Health Act, 1987 governs the law relating to the treatment and

Name	Brief features
Act, 1987	<p>care of mentally ill persons. It entails:</p> <ul style="list-style-type: none"> <li>- Power to Inspect records: Inspecting officers authorized by the State Government or by the licensing authority</li> <li>- Confidentiality of Inspection: Under what circumstances, personal records and health information of a patient so inspected could be disclosed</li> <li>- Visitor Log: Standards governing the data retention, security and access regarding the book and its contents do not exist.</li> </ul>
The Persons with Disabilities, (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995	<p>The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995 provides for education, employment, creation of a barrier free environment, social security, etc.</p> <ul style="list-style-type: none"> <li>- Disability Certificates: require sensitive and personal information to be provided</li> <li>- Collection : collection, compilation and analysis of data relating to socio-economic conditions of persons with disabilities</li> <li>- Employment : Special Employment Exchange collects and makes available employment information, in registers.</li> <li>- Access to Employment Registers by authorised person</li> <li>- Consent for Research : required from the individual or family members or caregiver's.</li> </ul>
Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994	<p>Salient features of the Act that pertain to privacy include:</p> <ul style="list-style-type: none"> <li>- Data Retention: records of pregnant women to be preserved for a period of two years</li> <li>- Mandatory provision of information: age, abortion history, and family history</li> </ul>
Medical Termination of Pregnancy Act, 1971	<p>The Medical Termination of Pregnancy Act, 1971 mandates abortion by a registered medical practitioner under stipulated conditions. Salient features of the Act that pertain to privacy include:</p> <ul style="list-style-type: none"> <li>- Consent : medical practitioner must collect documents indicating consent</li> <li>- Disclosure : only allowed to disclose information to Chief Medical Officer; otherwise, it prohibits the disclosure of matters</li> <li>- Data Processing : explicitly mandates data collection and processing</li> </ul>

Name	Brief features
Ethical Guidelines for Biomedical Research on Human Subjects	<p>The provisions for the regulation of privacy pertaining to biomedical research include aspects of consent as well as a limitation on the information that may be collected and its subsequent use.</p> <p>The provisions of this act aim to regulate the protection of privacy during clinical trials and during other methods of research.</p> <p>The principle of informed consent is an integral part of this set of guidelines.</p> <p>The Privacy related information included in the participant/ patient information sheet includes: the choice to prevent the use of their biological sample, the extent to which confidentiality of records could be maintained and the consequences of breach of confidentiality, possible current and future uses of the biological material and of the data to be generated from the research and if the material is likely to be used for secondary purposes or would be shared with others, the risk of discovery of biologically sensitive information and publications, including photographs and pedigree charts.</p> <p>The Guidelines require special concern for privacy and confidentiality when conducting genetic family studies. The protection of privacy and maintenance of confidentiality, specifically surrounding the identity and records, is maintained when using the information or genetic material provided by participants for research purposes.</p> <p>The Guidelines require investigators to maintain confidentiality of epidemiological data due to the particular concern that some population based data may also have implications on issues like national security or public safety.</p>
Insurance Regulatory and Development Authority (Third Party Administrators) Health Services Regulations, 2001	<p>The provisions of the Act regulate the practices of third party administrators within the healthcare sector so as to ensure their compliance with the basic principles of privacy.</p> <p>An exception to the maintenance and confidentiality of information confidentiality clause in the code of conduct, requires TPAs to provide relevant information to any Court of Law/Tribunal, the Government, or the Authority in the case of any investigation carried out or proposed to be carried out by the Authority against the insurance company, TPA or any other person or for any other reason..</p> <p>In July 2010, the IRDA notified the Insurance Regulatory and Development Authority (Sharing of Database for Distribution of Insurance Products) Regulations. These regulations restrict referral companies from providing details of their customers without their prior consent.</p>

Name	Brief features
	<p>TPAs must maintain the confidentiality of the data collected by it in the course of its agreement and maintain proper records of all transactions carried out by it on behalf of an insurance company and are also required to refrain from trading information and the records of its business.</p> <p>TPA's must keep records for a period of not less than three years.</p>
Information Technology Act, 2000	<p>The Information Technology Act, 2000 (IT Act) provides legal recognition to any transaction, which is done by electronic way or use of Internet. The issue of data protection has been addressed in Information Technology Amendment Act, 2008.</p> <p>It protects private information that is obtained by agencies by virtue of powers conferred under the Act.</p> <ul style="list-style-type: none"> <li>- Personal information is defined as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a corporate entity, is capable of identifying such person.</li> <li>- Sensitive personal data or information is defined as "personal information" which consists of information relating to any of the following: passwords; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to any of the above as provided to a corporate entity for providing service; and any of the information received under the above by a corporate entity for processing, stored or processed under lawful contract or otherwise. Data or information is not sensitive and personal if it is available in the public domain or furnished under the Right to Information Act of 2005.</li> </ul> <p>According to this Act:</p> <ul style="list-style-type: none"> <li>- Persons and organizations which store personal data must register with the Information commissioner, appointed as the government official to oversee the Act.</li> <li>- Restriction on collection of data: Personal data can be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.</li> <li>- The personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.</li> </ul>
<b>International Experience</b>	



- 4.1. Different countries have taken different approaches and mechanism to address issues pertaining to health data privacy and security. A summary on health data privacy & security related Acts of select countries like US, UK, Canada, Australia, Sweden, Singapore etc. has been given as below.

Country	Legislation / Act	Brief (objective, key elements etc.)
United States of America	Health Insurance Portability and Accountability Act of 1996 ("HIPAA")	<ul style="list-style-type: none"> <li>○ <u>Purpose</u>: To improve the portability of health insurance coverage; combat waste, fraud and abuse; and simplify health care administration. It requires development of a health information system through the establishment of standards &amp; requirements for the electronic transmission of certain health information.</li> <li>○ <u>HIPAA Privacy Rule &amp; Security Rule</u> : applicable to the privacy &amp; security of EPHRs (electronic personal health records).</li> <li>○ <u>HIPPA Privacy rule</u> institutes business processes to protect the use and disclosure of protected health information (PHI) i.e. individually identifiable health information in paper, electronic, or oral form</li> <li>○ <u>HIPAA Security Rule</u> : designed to provide protection for all individually identifiable health information that is maintained, transmitted or received in electronic form.</li> </ul> <p>Apart from the HIPAA, approximately 60 laws related to privacy in the healthcare sector have been enacted in more than 34 states. These legislations have been instrumental in creating awareness about privacy requirements in the healthcare sector and improving the efficiency of data collection and transfer.</p>
Canada	<ul style="list-style-type: none"> <li>• Privacy Act; Personal Information Protection and Electronic Documents Act;</li> <li>• Personal Health Information Protection Act, Ontario (PHIPA)</li> <li>• Personal Health Information Act, Nova Scotia</li> <li>• Personal Health</li> </ul>	<p>Privacy legislation in Canada can be grouped into four categories:</p> <ul style="list-style-type: none"> <li>○ <u>The Privacy Act</u>: Federal legislation directing the protection of personal information in government and other tax funded organizations. The Privacy Act limits the collection, use and disclosure of information by governmental entities and grants individuals' rights of access and correction of erroneous information.</li> <li>○ <u>Personal Information Protection and Electronic Documents Act (PIPEDA)</u>: Federal legislation directing the protection of personal information in private sector organizations. PIPEDA does not cover all personal information; companies in certain provinces are covered by provincial legislation.</li> </ul>

Country	Legislation / Act	Brief (objective, key elements etc.)
	Information Act, Manitoba • Personal Information Protection Act ('PIPA Alberta') • Health Information Act, Alberta	<ul style="list-style-type: none"> <li>◦ <u>Provincial legislation</u> : covers businesses operating in province &amp; must be formally pronounced to be substantially similar to the federal legislation; otherwise the federal legislation will supersede it.</li> <li>◦ <u>Health information legislation</u> : covers all personal information collected, used, and disclosed by the health system.</li> </ul> <p>Individuals must consent to the collection, use and disclosure of personal information.</p>
EU	• EU data protection regulation	<ul style="list-style-type: none"> <li>◦ The regulation calls for Privacy Impact Assessments when there are specific risks to privacy which would include profiling, sensitive data related to health, genetic material or biometric information.</li> <li>◦ The regulation also establishes the need for explicit consent for sensitive personal data. The regulation prohibits the use of data collected for an additional purpose, other than the purpose for which it was collected.</li> <li>◦ Embedded within the regulation is the right to be forgotten wherein patients can request for their data to be deleted after they have been discharged or the clinical trial has been concluded.</li> <li>◦ The regulation covers data that may be transferred outside the EEA, unless there is an additional level of data protection. If a court located outside the EU makes a request for the disclosure of personal data, prior authorization must be obtained from the local data protection authority before such transfer is made. It is imperative that this be implemented within Indian legislation as currently there is no mechanism to regulate the cross border transfer of personal data.</li> <li>◦ The consent obtained during a clinical trial may not always be sufficient to cover additional research even in instances of data being coded adequately. Thus, it may not be possible to anticipate additional research while carrying out initial research. The regulation prohibits the use of data collected for an additional purpose, other than the purpose for which it was collected.</li> </ul>
United Kingdom	• UK Data Protection Act - 1998	<ul style="list-style-type: none"> <li>◦ UK is a signatory to the European Union Directive on Data Privacy and a member of the European Economic Area (EEA). The UK's national enabling legislation is the Data</li> </ul>

Country	Legislation / Act	Brief (objective, key elements etc.)
		Protection Act of 1998.
Australia	• Privacy Act of 1988 (the "Act").	<ul style="list-style-type: none"><li>◦ The Privacy Amendment (Enhancing Privacy Protection) Act 2012 containing significant amendments to the Act came into effect on March 12, 2014.</li><li>◦ The provisions are in keeping with the 13 National Privacy Principles that represent the minimum standards of privacy regulation with respect to the handling of personal information in the healthcare sector.</li></ul>
Other countries		<ul style="list-style-type: none"><li>◦ Austria - Austrian Data Protection Act 2000 ("DSG")</li><li>◦ Estonia - Estonian Personal Data Protection Act</li><li>◦ Singapore - Singapore's Personal Data Protection Act 2012 ("PDPA")</li><li>◦ Czech Republic- Law on Care of People's Health</li><li>◦ Sweden- Personal Data Act</li><li>◦ Norway - Personal Data Act and the Personal Data Regulations</li></ul>

**Conclusion**

- 4.1. Under the current scenario and keeping in view the plans for large scale adoption of IT in Healthcare, need for a statute specifically protecting health data privacy & security aspects in a comprehensive manner is quite prominent as brought forward by the stakeholders at various platforms in the past. The Legal Sub-group constituted under EMR/EHR Standards Committee of MoHFW has decided to address health data privacy & security through an Act.
- 4.2. Since already there are different legislations/Acts specific to particular health conditions/circumstances, the envisaged Act needs to be comprehensively in sync with the existing provisions under other enactments — inconsistencies or conflict should be addressed. Also the provisions under IT Act, 2000 should be evaluated and appropriately incorporated/referred to.
- 4.3. Learning should also be drawn from the experiences of other countries like US, UK, Canada, Australia, Sweden, Singapore etc.

**Annexure I : Table of Content for the proposed Act to cover privacy & security aspects in Healthcare**

- I. Introduction**
  - a. Purposes of the Act
  - b. Scope of the Act
  - c. Inconsistencies or conflict with other enactments
- II. Definitions**
  - a. Anonymisation
  - b. Associate
  - c. Confidentiality
  - d. Consent
  - e. Custodian
  - f. De-identification
  - g. Electronic medical record (EMR)
  - h. Electronic health record (HER)
  - i. Electronic personal / protected health information (ePHI)
  - j. General health information
  - k. Guardian
  - l. Health information exchange
  - m. Information breach
  - n. Inadvertent information breach
  - o. Owner
  - p. Personal health record (PHR)
  - q. Personally identifiable health information
  - r. Privacy
  - s. Protected health information (PHI)

t. Public health information

u. Secrecy

v. Security

w. Sensitive information

x. System vendors

y. Wilful information breach

### **III. Collection & Storage of Health Information**

#### **a. Consent**

i. Types

ii. Consent-taking methodology

iii. Revocation methodology

iv. Methodology to deal with data released in the time between granting of consent and its revocation

#### **b. Collection & Purpose limitation**

#### **c. Rights related to request for individual health information**

i. Who can request?

ii. What can be requested?

iii. Who can request what?

iv. Under what circumstances can these requests be made?

v. What would be the mechanism to make a request?

vi. What would be the mechanism to abandon a request?

vii. What would be the mechanism to assist a person making the request?

viii. What would be the time limit for responding to such a request?

ix. Can the request be denied?

x. Under what circumstances can the request be denied?

xi. What would be the mechanism of denial?

xii. What would be the mechanism to seek redress in cases of denial?

## d. Amendments to records

- i. Who can make the request?
- ii. Who can make the amendments?
- iii. Who will authenticate such amendments?
- iv. Who may review the amendments?
- v. What would be time limit for responding to such requests?
- vi. Can such requests be denied?
- vii. What would be the mechanism of such denial?
- viii. What would be the mechanism to seek redress in such cases?

## e. Collection of public health information

- i. What is the method for collecting such information?
- ii. What is the justification for collecting such information?
- iii. What would be the mechanism for collecting such information?

## f. Collection of general health information

- i. What will constitute "general health information"?
- ii. What will be the mechanism for making such requests?
- iii. Who can make the request?
- iv. What all can be requested?
- v. Who can request what?
- vi. Under what circumstances can these requests be made?
- vii. What would be the mechanism to make a request?
- viii. What would be the mechanism to abandon a request?
- ix. What would be the mechanism to assist a person making the request?
- x. What would be the time limit for responding to such a request?
- xi. Can the request be denied?
- xii. Under what circumstances can the request be denied?

- xiii. What would be the mechanism of denial?
- xiv. What would be the mechanism to seek redress in cases of denial?

#### IV. Exchange & Use of Health Information

##### a. Use of health information

- i. What can be used?
- ii. What all are completely prohibited?
- iii. What all are generally prohibited but may be used under special circumstances?
- iv. What would constitute a special circumstance?
- v. What can be used for research purposes?
- vi. What is the methodology for using information for research purposes?

##### b. Distribution and sharing of health information

###### i. Distribution of information

###### 1. Free distribution

- a. What can be distributed freely?
- b. To whom may the information be distributed freely?

###### 2. Restricted distribution

- a. What can be distributed with restriction?
- b. What might these restrictions be?
- c. To whom may the information distributed to with restriction?

###### ii. Sharing of information

###### 1. Free sharing

- a. What information can be shared freely?
- b. With whom may the information be shared with freely?

###### 2. Restricted sharing

- a. What would be considered as "restricted sharing"?

b. What information can be shared?

c. What will be the methodology of restricted sharing?

**V. Security**

a. Purpose of the Security Standards

b. Technical Standards

i. Access control & privileges

ii. Audit log

iii. Integrity

iv. Authentication

v. Encryption

c. Administrative Safeguards Standards

d. Physical Safeguards Standards

**VI. Duties and responsibilities**

a. Owner

b. Custodian

c. Guardian

d. Associate

**VII. Information breach**

a. Penalties

i. Wilful information breach

ii. Inadvertent information breach

b. Immunities

i. Owners

ii. Custodians

iii. Guardians

iv. System vendors



- v. Third party with whom information has been shared
- c. Filing of complaint
  - i. Who can complain?
  - ii. What supporting evidence should be present for the complaint to be taken cognizance of?
  - iii. Complaint methodology
    - 1. What would the process be for filing of complaint?
    - 2. Can *suo moto* cognizance be taken without any formal complaint?
    - 3. To whom can the complaint be made?
    - 4. How may action be initiated by the appropriate authority?

#### VIII. Appeal

- a. Appellate authorities
  - i. Conflict of Interest / Adjudicator
  - ii. Law courts
- b. Appellate methodology
- c. Methodology for leave to appeal to the appropriate authority

#### IX. National eHealth Authority (NeHA)

- a. Statutory body for ensuring implementation of the privacy & security provisions as per the Act & promoting setting-up of Health Information Exchange

#### X. Establishment of Health Information Exchanges in each State and at Central level

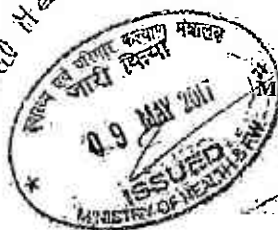
#### XI. Formulation of rules

#### XII. Removal of inconsistencies with other enactments

**Annexure II :****Concept Note on setting up of National eHealth Authority (NeHA)**

641925/2017/E-GOVERNANCE

Parliamentary Matter  
Most Immediate  
By Special Messenger



File No. H-11016/1/2015-eGov  
Government of India  
Ministry of Health & Family Welfare  
(eHealth Section)  
\*\*\*\*\*

Nirman Bhawan, New Delhi  
Dated 9<sup>th</sup> May, 2017

**OFFICE MEMORANDUM**

Subject: Assurance given on 24/04/2015 in reply to Lok Sabha USQ No. 5250-reg.

Reference is invited to this Ministry's O.M. of even number dated 06.12.2016 on the aforementioned subject and to say that current status of Assurance given on 24.04.2015 in reply to Lok Sabha USQ no. 5250 is as follows:-

"A concept note of NeHA was prepared and National consultation was held on 4th April, 2016; Establishment of National e-Health Authority (NeHA) is clubbed with Health Data Privacy & Security Act. Recently, a draft of legislation prepared by National Law School of India University (NLSIU), Bengaluru has been discussed on 24<sup>th</sup> March 2017. Key suggestions made by participants and legal experts have been noted and the draft is being revised accordingly."

2. Since it will take some more time to complete the formalities and finalize the National e-Health Authority, the Committee on Government Assurance, Lok Sabha may be requested to kindly grant extension for 6 months till 24<sup>th</sup> October, 2017 for the purpose of fulfilling the above assurance.

3. This issue with the approval of Hon'ble Minister of State for Health & Family Welfare.

(S.K. Panig)

Under Secretary, MoHFW  
011-23061213

The Committee on Government Assurances  
Lok Sabha Secretariat  
Parliament House Annexe,  
New Delhi

**Copy for information & necessary action to:**

1. Ministry of Parliament Affairs, Deputy Secretary (Impl. I section), 92, Parliament House, New Delhi.
2. Parliament Section, M/o Health & Family Welfare, Nirman Bhawan, New Delhi.

AV  
9/5/17

लोक सभा का XVI-IV सत्र, 2015 File No.H-11016/1/2015-eGov  
 Receipt No : 374878/2016/E-GOV

18

मंत्रालय स्वास्थ्य और परिवार कल्याण विभाग स्वास्थ्य और परिवार कल्याण

XVI-IV

Session of Lok Sabha, 2015

Ministry of HEALTH AND FAMILY WELFARE

Date of fulfillment

Department of HEALTH AND FAMILY WELFARE

प्रश्न सं० और तारीख Q.No. & Date	विषय Subject	दिया गया व श्वासना Promise Made	कब और कैसे पूरा किया गया When & How Fulfilled	अभ्युक्ति/ Reime विलम्ब के कारण Reasons for De.
1	2	3	4	5
UNSTARRED Q.NO. 5250  अंतरासक्ति प्रश्न संख्या 5250 24-04-2015  by Shri Suvendu Adhikari, Dr. Manoj Rajoria, Shri A. Arunmozhi van, Shri R. Dhruva Narayana	NATIONAL E HEALTH AUTHORITY  Asking for :-  (a) whether the Government proposes to centralise medical history of patients for easy access of hospitals and laboratories under National e-Health Authority, if so, the details thereof;  (b) whether this initiative is likely to allow healthcare professionals access to complete and accurate health history for better diagnosis and treatment without compromising on patient confidentiality; and  (c) if so, details thereof including the role likely to be played by the States in its implementation and the expenditure likely to be incurred thereon?	(b) to (c): Establishment of National e-Health Authority (NeHA) is at a concept stage, as of now and views/ suggestions from various stakeholders including the States have been invited on the Concept Note of NeHA.		

GOVERNMENT OF INDIA  
MINISTRY OF HEALTH AND FAMILY WELFARE  
DEPARTMENT OF HEALTH AND FAMILY WELFARE

LOK SABHA

UNSTARRED QUESTION NO. 5250  
TO BE ANSWERED ON 24<sup>TH</sup> APRIL, 2015

NATIONAL E-HEALTH AUTHORITY

5250. SHRI SUVENDU ADHIKARI:

SHRI A. ARUNMOZHITHEVAN:

SHRI R. DHRUVA NARAYANA:

DR. MANOJ RAJORIA:

Will the Minister of HEALTH AND FAMILY WELFARE be pleased to state:

- (a) whether the Government proposes to centralise medical history of patients for easy access of hospitals and laboratories under National e-Health Authority; if so, the details thereof;
- (b) whether this initiative is likely to allow healthcare professionals access to complete and accurate health history for better diagnosis and treatment without compromising on patient confidentiality;
- (c) if so, details thereof including the role likely to be played by the States in its implementation and the expenditure likely to be incurred thereon; and
- (d) whether the Government proposes to launch any National Health programme under PPP model and develop the spectrum of telemedicine to strengthen the healthcare system of the country and if so, the details thereof?

ANSWER

THE MINISTER OF HEALTH AND FAMILY WELFARE  
(SHRI JAGAT PRAKASH NADDA)

(a): No.

(b) to (c): Establishment of National e-Health Authority (NeHA) is at a concept stage, as of now and views/suggestions from various stakeholders including the States have been invited on the Concept Note of NeHA.

Receipt No. 374878/2016/E-GOV

File No. H-11016/1/2015-eGov

10

It is proposed that NeHA will promote standardization of Electronic Health Records (EHRs) & establishment of Health Information Exchanges (HIEs). It is envisioned that states will establish Health Information Exchanges, which will facilitate exchange of EHRs across facilities in a secured manner. States may also establish EHR stores/repositories. A detailed project report (DPR) has been prepared by this Ministry for establishment of pan-India Integrated Health Information System including EHR System in public health care facilities and establishment of Health Information Exchanges (HIE) at National & State levels under National e-Governance Plan (e-Kranti). The projected outlay of this project is Rs. 8,400 Crores (approximately) over a duration of seven years including States' share.

(d) No.

641925/2017/E-GOVERNANCE

File No. H-11016/10/2016-e-Health

Government of India  
Ministry of Health & Family Welfare  
(e-Health Division)

सुईड पोस्ट द्वारा  
BY SPEED POST

Nirman Bhawan, New Delhi  
Dated 23 February, 2017

OFFICE MEMORANDUM

Subject: Assurance given on 25/11/2016 in reply to USQ No-1639-reg.

The undersigned is directed to refer to Lok Sabha Secretariat OM.No XVI-X/H&FW(4)/USQ/1639-LS/2016 dated 20.12.2016 on the above mentioned subject and to say that, the work of drafting the proposed legislation for Health Data Privacy & Security Act, was awarded to National Law School of India University (NLSIU), Bengaluru. The draft of the legislation is ready and is under consideration in the Ministry."

2. Since it will take some more time to complete the formalities and finalize the proposed legislation, the Committee on Government Assurance, Lok Sabha may be requested to kindly grant extension till 25<sup>th</sup> August, 2017 for the purpose of fulfilling the above assurance.

3. This issues with the approval of Hon'ble Minister of Health & Family Welfare.

(Jitendra Arora)  
Director(e-Health)  
Tel: 23062317

To

The Committee on Government Assurances  
Lok Sabha Secretariat  
Parliament House Annexe,  
New Delhi

Copy for information & necessary action to:

1. Ministry of Parliament Affairs, Deputy Secretary (Impl. I section), 92, Parliament House, New Delhi.
2. Parliament Section, M/o Health & Family Welfare, Nirman Bhawan, New Delhi

*Ar*  
24/2/17

641925/2017/E-GOVERNANCE

2016

स्वास्थ्य और परिवार कल्याण

विभाग

स्वास्थ्य और परिवार कल्याण

पूर्ति की तारीख

X

Session of Lok Sabha, 2016

Ministry of HEALTH AND FAMILY WELFARE

Department of HEALTH AND FAMILY WELFARE

Date of fulfillment

प्रश्न सं० और तारीख Q.No. & Date	विषय Subject	दिया गया आश्वासन Promise Made	कब और कैसे पूरा किया गया When & How Fulfilled	अभिव्यक्ति/ Remark विलम्ब के कारण Reasons for Delay
1	2	3	4	5
UNSTARRED Q.NO. 1639 अतारांकित प्रश्न संख्या 1639 25-11-2016 by: Shri R. Gopalakrishnan, Shri Suresh Chanabasappa Angadi	SAFEGUARDING PATIENTS PRIVACY  Asking for :-  (a) whether the Government proposes to bring out a legislation to safeguard patient's privacy by protecting health data and medical information of patients;  (b) if so, the details thereof;  (c) whether the said legislation has provisions for action against any breach of data of the patients; and  (d) if so, the details thereof and if not, the reasons therefor?	(c) & (d): Yes. However, the proposed legislation is still being drafted and action against any breach of electronic data of the patients are yet to be finalized.		



GOVERNMENT OF INDIA  
MINISTRY OF HEALTH AND FAMILY WELFARE  
DEPARTMENT OF HEALTH AND FAMILY WELFARE

LOK SABHA  
UNSTARRED QUESTION NO.1639  
TO BE ANSWERED ON 25<sup>TH</sup> NOVEMBER, 2016

SAFEGUARDING PATIENTS PRIVACY

1639. SHRI R. GOPALAKRISHNAN:  
SHRI SURESH C. ANGADI:

Will the Minister of HEALTH AND FAMILY WELFARE be pleased to state:

- (a) whether the Government proposes to bring out a legislation to safeguard patient's privacy by protecting health data and medical information of patients;
- (b) if so, the details thereof;
- (c) whether the said legislation has provisions for action against any breach of data of the patients; and
- (d) if so, the details thereof and if not, the reasons therefor?

ANSWER  
THE MINISTER OF STATE IN THE MINISTRY OF HEALTH AND  
FAMILY WELFARE  
(ANUPRIYA PATEL)

(a) & (b): Yes. Ministry has decided to bring out a legislation regarding Electronic Health Data, Privacy and Security. The proposed legislation will broadly cover the following aspects :

1. Comprehensive legal framework to protect 'e-health data' of an 'individual'.
2. Ownership of 'e-health data'.
3. Legal framework for health data standardization in collection, storage, exchange etc.
4. Comprehensive remedies (civil and criminal) for data breach.
5. Enforcing nodal body.

(c) & (d): Yes. However, the proposed legislation is still being drafted and action against any breach of electronic data of the patients are yet to be finalized.

The draft



सत्यमेव जयते

**Ministry of Health and Family Welfare  
Government of India**

**NATIONAL HEALTH POLICY, 2017**

<b>Contents</b>		
<b>1</b>	<b>Introduction:</b>	<b>1</b>
<b>2</b>	<b>Goal, Principles and Objectives</b>	<b>1</b>
2.1	Goal	1
2.2	Key Policy Principles	1
2.3	Objectives	3
2.4	Specific Quantitative Goals and Objectives	3
<b>3</b>	<b>Policy Thrust</b>	<b>6</b>
3.1	Ensuring Adequate Investment	6
3.2	Preventive and Promotive Health	6
3.3	Organisation of Public Health Care Delivery	7
3.3.1	Primary Care Services & Continuity of Care	8
3.3.2	Secondary Care Services	9
3.3.3	Reorienting Public Hospitals	10
3.3.4	Closing Infrastructure and Human Resource/Skill Gaps	10
3.3.5	Urban Health Care	10
4.1	RMNCH+A services	11
4.2	Child and Adolescent Health	11
4.3	Interventions to address malnutrition and micronutrient deficiencies	11
4.4	Universal Immunisation	12
4.5	Communicable Diseases	12
4.6	Non Communicable Diseases	13
4.7	Mental Health	13
4.8	Population Stabilisation	13
<b>5</b>	<b>Women's Health and Gender Mainstreaming</b>	<b>14</b>
<b>6</b>	<b>Gender Based Violence</b>	<b>14</b>
<b>7</b>	<b>Supportive supervision</b>	<b>14</b>
<b>8</b>	<b>Emergency Care and Disaster Preparedness</b>	<b>14</b>
<b>9</b>	<b>Mainstreaming the potential of AYUSH</b>	<b>14</b>
<b>10</b>	<b>Tertiary Care Services</b>	<b>15</b>
<b>11</b>	<b>Human Resources for Health</b>	<b>15</b>
<b>12</b>	<b>Financing of Health Care</b>	<b>18</b>
<b>13</b>	<b>Collaboration with Non-Government Sector/Engagement with private sector</b>	<b>19</b>
<b>14</b>	<b>Regulatory Framework</b>	<b>22</b>
<b>15</b>	<b>Vaccine Safety</b>	<b>24</b>
<b>16</b>	<b>Medical Technologies</b>	<b>24</b>
<b>17</b>	<b>Public Procurement</b>	<b>24</b>
<b>18</b>	<b>Availability of Drugs and Medical Devices</b>	<b>24</b>

19	Aligning other policies for medical devices and equipment with public health goals	24
20	Improving Public Sector Capacity for manufacturing essential drugs and vaccines	24
21	Anti-microbial Resistance	25
22	Health Technology Assessment	25
23	Digital Health Technology Eco - System	25
24	Health Surveys	25
25	Health Research	26
26	Governance	27
27	Legal Framework for Health Care and Health Pathway	27
28	Implementation Framework and Way forward	28

## 1. Introduction

The National Health Policy of 1983 and the National Health Policy of 2002 have served well in guiding the approach for the health sector in the Five-Year Plans. Now 14 years after the last health policy, the context has changed in four major ways. First, the health priorities are changing. Although maternal and child mortality have rapidly declined, there is growing burden on account of non-communicable diseases and some infectious diseases. The second important change is the emergence of a robust health care industry estimated to be growing at double digit. The third change is the growing incidences of catastrophic expenditure due to health care costs, which are presently estimated to be one of the major contributors to poverty. Fourth, a rising economic growth enables enhanced fiscal capacity. Therefore, a new health policy responsive to these contextual changes is required.

The primary aim of the National Health Policy, 2017, is to inform, clarify, strengthen and prioritize the role of the Government in shaping health systems in all its dimensions- investments in health, organization of healthcare services, prevention of diseases and promotion of good health through cross sectoral actions, access to technologies, developing human resources, encouraging medical pluralism, building knowledge base, developing better financial protection strategies, strengthening regulation and health assurance.

NHP 2017 builds on the progress made since the last NHP 2002. The developments have been captured in the document “Backdrop to National Health Policy 2017- Situation Analyses”, Ministry of Health & Family Welfare, Government of India.

## 2. Goal, Principles and Objectives

### 2.1 Goal

The policy envisages as its goal the attainment of the highest possible level of health and well-being for all at all ages, through a preventive and promotive health care orientation in all developmental policies, and universal access to good quality health care services without anyone having to face financial hardship as a consequence. This would be achieved through increasing access, improving quality and lowering the cost of healthcare delivery.

The policy recognizes the pivotal importance of Sustainable Development Goals (SDGs). An indicative list of time bound quantitative goals aligned to ongoing national efforts as well as the global strategic directions is detailed at the end of this section.

### 2.2 Key Policy Principles

- I. **Professionalism, Integrity and Ethics:** The health policy commits itself to the highest professional standards, integrity and ethics to be maintained in the entire system of health care

delivery in the country, supported by a credible, transparent and responsible regulatory environment.

- II. **Equity:** Reducing inequity would mean affirmative action to reach the poorest. It would mean minimizing disparity on account of gender, poverty, caste, disability, other forms of social exclusion and geographical barriers. It would imply greater investments and financial protection for the poor who suffer the largest burden of disease.
- III. **Affordability:** As costs of care increases, affordability, as distinct from equity, requires emphasis. Catastrophic household health care expenditures defined as health expenditure exceeding 10% of its total monthly consumption expenditure or 40% of its monthly non-food consumption expenditure, are unacceptable.
- IV. **Universality:** Prevention of exclusions on social, economic or on grounds of current health status. In this backdrop, systems and services are envisaged to be designed to cater to the entire population- including special groups.
- V. **Patient Centered & Quality of Care:** Gender sensitive, effective, safe, and convenient healthcare services to be provided with dignity and confidentiality. There is need to evolve and disseminate standards and guidelines for all levels of facilities and a system to ensure that the quality of healthcare is not compromised.
- VI. **Accountability:** Financial and performance accountability, transparency in decision making, and elimination of corruption in health care systems, both in public and private.
- VII. **Inclusive Partnerships:** A multistakeholder approach with partnership & participation of all non-health ministries and communities. This approach would include partnerships with academic institutions, not for profit agencies, and health care industry as well.
- VIII. **Pluralism:** Patients who so choose and when appropriate, would have access to AYUSH care providers based on documented and validated local, home and community based practices. These systems, inter alia, would also have Government support in research and supervision to develop and enrich their contribution to meeting the national health goals and objectives through integrative practices.
- IX. **Decentralization:** Decentralisation of decision making to a level as is consistent with practical considerations and institutional capacity. Community participation in health planning processes, to be promoted side by side.
- X. **Dynamism and Adaptiveness:** constantly improving dynamic organization of health care based on new knowledge and evidence with learning from the communities and from national and international knowledge partners is designed.

## 2.3 Objectives

Improve health status through concerted policy action in all sectors and expand preventive, promotive, curative, palliative and rehabilitative services provided through the public health sector with focus on quality.

### 2.3.1 Progressively achieve Universal Health Coverage

A. Assuring availability of free, comprehensive primary health care services, for all aspects of reproductive, maternal, child and adolescent health and for the most prevalent communicable, non-communicable and occupational diseases in the population. The Policy also envisages optimum use of existing manpower and infrastructure as available in the health sector and advocates collaboration with non-government sector on pro-bono basis for delivery of health care services linked to a health card to enable every family to have access to a doctor of their choice from amongst those volunteering their services.

B. Ensuring improved access and affordability, of quality secondary and tertiary care services through a combination of public hospitals and well measured strategic purchasing of services in health care deficit areas, from private care providers, especially the not-for profit providers

C. Achieving a significant reduction in out of pocket expenditure due to health care costs and achieving reduction in proportion of households experiencing catastrophic health expenditures and consequent impoverishment.

**2.3.2 Reinforcing trust in Public Health Care System:** Strengthening the trust of the common man in public health care system by making it predictable, efficient, patient centric, affordable and effective, with a comprehensive package of services and products that meet immediate health care needs of most people.

**2.3.3 Align the growth of private health care sector with public health goals:** Influence the operation and growth of the private health care sector and medical technologies to ensure alignment with public health goals. Enable private sector contribution to making health care systems more effective, efficient, rational, safe, affordable and ethical. Strategic purchasing by the Government to fill critical gaps in public health facilities would create a demand for private health care sector, in alignment with the public health goals.

**2.4 Specific Quantitative Goals and Objectives:** The indicative, quantitative goals and objectives are outlined under three broad components viz. (a) health status and programme impact, (b) health systems performance and (c) health system strengthening. These goals and objectives are aligned to achieve sustainable development in health sector in keeping with the policy thrust.

## 2.4.1 Health Status and Programme Impact

### 2.4.1.1 *Life Expectancy and healthy life*

- a. Increase Life Expectancy at birth from 67.5 to 70 by 2025.
- b. Establish regular tracking of Disability Adjusted Life Years (DALY) Index as a measure of burden of disease and its trends by major categories by 2022.
- c. Reduction of TFR to 2.1 at national and sub-national level by 2025.

### 2.4.1.2 *Mortality by Age and/ or cause*

- a. Reduce Under Five Mortality to 23 by 2025 and MMR from current levels to 100 by 2020.
- b. Reduce infant mortality rate to 28 by 2019.
- c. Reduce neo-natal mortality to 16 and still birth rate to “single digit” by 2025.

### 2.4.1.3 *Reduction of disease prevalence/ incidence*

- a. Achieve global target of 2020 which is also termed as target of 90:90:90, for HIV/AIDS i. e., - 90% of all people living with HIV know their HIV status, - 90% of all people diagnosed with HIV infection receive sustained antiretroviral therapy and 90% of all people receiving antiretroviral therapy will have viral suppression.
- b. Achieve and maintain elimination status of Leprosy by 2018, Kala-Azar by 2017 and Lymphatic Filariasis in endemic pockets by 2017.
- c. To achieve and maintain a cure rate of >85% in new sputum positive patients for TB and reduce incidence of new cases, to reach elimination status by 2025.
- d. To reduce the prevalence of blindness to 0.25/ 1000 by 2025 and disease burden by one third from current levels.
- e. To reduce premature mortality from cardiovascular diseases, cancer, diabetes or chronic respiratory diseases by 25% by 2025.

## 2.4.2 Health Systems Performance

### 2.4.2.1 *Coverage of Health Services*

- a. Increase utilization of public health facilities by 50% from current levels by 2025.
- b. Antenatal care coverage to be sustained above 90% and skilled attendance at birth above 90% by 2025.
- c. More than 90% of the newborn are fully immunized by one year of age by 2025.
- d. Meet need of family planning above 90% at national and sub national level by 2025.



- e. 80% of known hypertensive and diabetic individuals at household level maintain ‘controlled disease status’ by 2025.

**2.4.2.2 Cross Sectoral goals related to health**

- a. Relative reduction in prevalence of current tobacco use by 15% by 2020 and 30% by 2025.
- b. Reduction of 40% in prevalence of stunting of under-five children by 2025.
- c. Access to safe water and sanitation to all by 2020 (Swachh Bharat Mission).
- d. Reduction of occupational injury by half from current levels of 334 per lakh agricultural workers by 2020.
- e. National/ State level tracking of selected health behaviour.

**2.4.3 Health Systems strengthening**

**2.4.3.1 Health finance**

- a. Increase health expenditure by Government as a percentage of GDP from the existing 1.15% to 2.5 % by 2025.
- b. Increase State sector health spending to > 8% of their budget by 2020.
- c. Decrease in proportion of households facing catastrophic health expenditure from the current levels by 25%, by 2025.

**2.4.3.2 Health Infrastructure and Human Resource**

- a. Ensure availability of paramedics and doctors as per Indian Public Health Standard (IPHS) norm in high priority districts by 2020.
- b. Increase community health volunteers to population ratio as per IPHS norm, in high priority districts by 2025.
- c. Establish primary and secondary care facility as per norms in high priority districts (population as well as time to reach norms) by 2025.

**2.4.3.3 Health Management Information**

- a. Ensure district-level electronic database of information on health system components by 2020.
- b. Strengthen the health surveillance system and establish registries for diseases of public health importance by 2020.
- c. Establish federated integrated health information architecture, Health Information Exchanges and National Health Information Network by 2025.

### 3. Policy Thrust

**3.1 Ensuring Adequate Investment** The policy proposes a potentially achievable target of raising public health expenditure to 2.5% of the GDP in a time bound manner. It envisages that the resource allocation to States will be linked with State development indicators, absorptive capacity and financial indicators. The States would be incentivised for incremental State resources for public health expenditure. General taxation will remain the predominant means for financing care. The Government could consider imposing taxes on specific commodities- such as the taxes on tobacco, alcohol and foods having negative impact on health, taxes on extractive industries and pollution cess. Funds available under Corporate Social Responsibility would also be leveraged for well-focused programmes aiming to address health goals.

**3.2 Preventive and Promotive Health** The policy articulates to institutionalize inter-sectoral coordination at national and sub-national levels to optimize health outcomes, through constitution of bodies that have representation from relevant non-health ministries. This is in line with the emergent international “Health in All” approach as complement to Health for All. The policy prerequisite is for an empowered public health cadre to address social determinants of health effectively, by enforcing regulatory provisions.

The policy identifies coordinated action on seven priority areas for improving the environment for health:

- The *Swachh Bharat Abhiyan*
- Balanced, healthy diets and regular exercises.
- Addressing tobacco, alcohol and substance abuse
- *Yatri Suraksha* – preventing deaths due to rail and road traffic accidents
- *Nirbhaya Nari* –action against gender violence
- Reduced stress and improved safety in the work place
- Reducing indoor and outdoor air pollution

The policy also articulates the need for the development of strategies and institutional mechanisms in each of these seven areas, to create *Swasth Nagrik Abhiyan* –a social movement for health. It recommends setting indicators, their targets as also mechanisms for achievement in each of these areas.

The policy recognizes and builds upon preventive and promotive care as an under-recognized reality that has a two-way continuity with curative care, provided by health agencies at same or at higher levels. The policy recommends an expansion of scope of interventions to include early detection and response to early childhood development delays and disability, adolescent and sexual health education, behavior change with respect to tobacco and alcohol use, screening, counseling for primary prevention and secondary prevention from common chronic illness –both communicable and non-communicable diseases. Additionally the policy focus is on extending coverage as also quality of

the existing package of services. Policy recognizes the need to frame and adhere to health screening guidelines across age groups. Zoonotic diseases like rabies need to be addressed through concerted and coordinated action, at the national front and through strengthening of the National Rabies Control Programme.

The policy lays greater emphasis on investment and action in school health- by incorporating health education as part of the curriculum, promoting hygiene and safe health practices within the school environs and by acting as a site of primary health care. Promotion of healthy living and prevention strategies from AYUSH systems and Yoga at the work-place, in the schools and in the community would also be an important form of health promotion that has a special appeal and acceptability in the Indian context.

Recognizing the risks arising from physical, chemical, and other workplace hazards, the policy advocates for providing greater focus on occupational health. Work-sites and institutions would be encouraged and monitored to ensure safe health practices and accident prevention, besides providing preventive and promotive healthcare services.

ASHA will also be supported by other frontline workers like health workers (male/female) to undertake primary prevention for non-communicable diseases. They would also provide community or home based palliative care and mental health services through health promotion activities. These workers would get support from local self-government and the Village Health Sanitation and Nutrition Committee (VHSNC).

In order to build community support and offer good healthcare to the vulnerable sections of the society like the marginalised, the socially excluded, the poor, the old and the disabled, the policy recommends strengthening the VHSNCs and its equivalent in the urban areas.

'Health Impact Assessment' of existing and emerging policies, of key non-health departments that directly or indirectly impact health would be taken up.

### **3.3 Organization of Public Health Care Delivery:** The policy proposes seven key policy shifts in organizing health care services

- In primary care – from selective care to assured comprehensive care with linkages to referral hospitals
- In secondary and tertiary care – from an input oriented to an output based strategic purchasing
- In public hospitals – from user fees & cost recovery to assured free drugs, diagnostic and emergency services to all
- In infrastructure and human resource development – from normative approach to targeted approach to reach under-serviced areas
- In urban health – from token interventions to on-scale assured interventions, to organize Primary Health Care delivery and referral support for urban poor. Collaboration with other sectors to address wider determinants of urban health is advocated.

- In National Health Programmes – integration with health systems for programme effectiveness and in turn contributing to strengthening of health systems for efficiency.
- In AYUSH services – from stand-alone to a three dimensional mainstreaming

Free primary care provision by the public sector, supplemented by strategic purchase of secondary care hospitalization and tertiary care services from both public and from non-government sector to fill critical gaps would be the main strategy of assuring healthcare services. The policy envisages strategic purchase of secondary and tertiary care services as a short term measure. Strategic purchasing refers to the Government acting as a single payer. The order of preference for strategic purchase would be public sector hospitals followed by not-for profit private sector and then commercial private sector in underserved areas, based on availability of services of acceptable and defined quality criteria. In the long run, the policy envisages to have fully equipped and functional public sector hospitals in these areas to meet secondary and tertiary health care needs of population, especially the poorest and marginalized. Public facilities would remain the focal point in the healthcare delivery system and services in the public health facilities would be expanded from current levels. The policy recognizes the special health needs of tribal and socially vulnerable population groups and recommends situation specific measures in provisioning and delivery of services. The policy advocates enhanced outreach of public healthcare through Mobile Medical Units (MMUs), etc. Tribal population in the country is over 100 million (Census 2011), and hence deserves special attention keeping in mind their geographical and infrastructural challenges. Keeping in view the high cost involved in provisioning and managing orphan diseases, the policy encourages active engagement with non-government sector for addressing the situation. In order to provide access and financial protection at secondary and tertiary care levels, the policy proposes free drugs, free diagnostics and free emergency care services in all public hospitals. To address the growing challenges of urban health, the policy advocates scaling up National Urban Health Mission (NUHM) to cover the entire urban population within the next five years with sustained financing.

For effectively handling medical disasters and health security, the policy recommends that the public healthcare system retain a certain excess capacity in terms of health infrastructure, human resources, and technology which can be mobilized in times of crisis.

In order to leverage the pluralistic health care legacy, the policy recommends mainstreaming the different health systems. This would involve increasing the validation, evidence and research of the different health care systems as a part of the common pool of knowledge. It would also involve providing access and informed choice to the patients, providing an enabling environment for practice of different systems of medicine, an enabling regulatory framework and encouraging cross referrals across these systems.

### **3.3.1 Primary Care Services and Continuity of Care:**

This policy denotes important change from very selective to comprehensive primary health care package which includes geriatric health care, palliative care and rehabilitative care services. The facilities which start providing the larger package of comprehensive primary health care will be called

'Health and Wellness Centers'. Primary care must be assured. To make this a reality, every family would have a health card that links them to primary care facility and be eligible for a defined package of services anywhere in the country. The policy recommends that health centres be established on geographical norms apart from population norms. To provide comprehensive care, the policy recommends a matching human resources development strategy, effective logistics support system and referral backup. This would also necessitate upgradation of the existing sub-centres and reorienting PHCs to provide comprehensive set of preventive, promotive, curative and rehabilitative services. It would entail providing access to assured AYUSH healthcare services, as well as support documentation and validation of local home and community based practices. The policy also advocates for research and validation of tribal medicines. Leveraging the potential of digital health for two way systemic linkages between the various levels of care viz., primary, secondary and tertiary, would ensure continuity of care. The policy advocates that the public health system would put in place a gatekeeping mechanism at primary level in a phased manner, accompanied by an effective feedback and follow-up mechanism.

### 3.3.2 Secondary Care Services:

The policy aspires to provide at the district level most of the secondary care which is currently provided at a medical college hospital. Basic secondary care services, such as caesarian section and neonatal care would be made available at the least at sub-divisional level in a cluster of few blocks. To achieve this, policy therefore aims:

- To have at least two beds per thousand population distributed in such a way that it is accessible within golden hour rule. This implies an efficient emergency transport system. The policy also aims that ten categories of what are currently specialist skills be available within the district. Additionally four or at least five of these specialist skill categories be available at sub-district levels. This may be achieved by strengthening the district hospital and a well-chosen, well located set of sub-district hospitals.
- Resource allocation that is responsive to quantity, diversity and quality of caseloads provided.
- Purchasing care after due diligence from non-Government hospitals as a short term strategy till public systems are strengthened.

Policy proposes a responsive and strong regulatory framework to guide purchasing of care from non-government sector so that challenges of quality of care, cost escalations and impediments to equity are addressed effectively.

In order to develop the secondary care sector, comprehensive facility development and obligations with regard to human resources, especially specialists needs, are to be prioritized. To this end the policy recommends a scheme to develop human resources and specialist skills.

Access to blood and blood safety has been a major concern in district healthcare services. This policy affirms in expanding the network of blood banks across the country to ensure improved access to safe blood.

### 3.3.3 Re-Orienting Public Hospitals:

Public hospitals have to be viewed as part of tax financed single payer health care system, where the care is pre-paid and cost efficient. This outlook implies that quality of care would be imperative and the public hospitals and facilities would undergo periodic measurements and certification of level of quality. The policy endorses that the public hospitals would provide universal access to a progressively wide array of free drugs and diagnostics with suitable leeway to the States to suit their context. The policy seeks to eliminate the risks of inappropriate treatment by maintaining adequate standards of diagnosis and treatment. Policy recognizes the need for an information system with comprehensive data on availability and utilization of services not only in public hospitals but also in non-government sector hospitals. State public health systems should be able to provide all emergency health services other than services covered under national health programmes.

### 3.3.4 Closing Infrastructure and Human Resources/Skill Gaps:

The policy duly acknowledges the roadmap of the 12th Five Year Plan for managing human resources for health. The policy initiatives aim for measurable improvements in quality of care. Districts and blocks which have wider gaps for development of infrastructure and deployment of additional human resources would receive focus. Financing for additional infrastructure or human resources would be based on needs of outpatient and inpatient attendance and utilization of key services in a measurable manner.

### 3.3.5 Urban Health Care:

National health policy prioritizes addressing the primary health care needs of the urban population with special focus on poor populations living in listed and unlisted slums, other vulnerable populations such as homeless, rag-pickers, street children, rickshaw pullers, construction workers, sex workers and temporary migrants. Policy would also prioritize the utilization of AYUSH personnel in urban health care. Given the large presence of private sector in urban areas, policy recommends exploring the possibilities of developing sustainable models of partnership with for profit and not for profit sector for urban health care delivery. An important focus area of the urban health policy will be achieving convergence among the wider determinants of health – air pollution, better solid waste management, water quality, occupational safety, road safety, housing, vector control, and reduction of violence and urban stress. These dimensions are also important components of smart cities. Healthcare needs of the people living in the peri urban areas would also be addressed under the NUHM. Further, Non-Communicable Diseases (NCDs) like hyper tension, diabetes which are predominant in the urban areas would be addressed under NUHM, through planned early detection. Better secondary prevention would also be an integral part of the urban health strategy. Improved health seeking behavior, influenced through capacity building of the community based organizations & establishment of an appropriate referral mechanism, would also be important components of this strategy.

#### 4. National Health Programmes

**4.1 RMNCH+A services:** Maternal and child survival is a mirror that reflects the entire spectrum of social development. This policy aspires to elicit developmental action of all sectors to support Maternal and Child survival. The policy strongly recommends strengthening of general health systems to prevent and manage maternal complications, to ensure continuity of care and emergency services for maternal health. In order to comprehensively address factors affecting maternal and child survival, the policy seeks to address the social determinants through developmental action in all sectors.

**4.2 Child and Adolescent Health:** The policy endorses the national consensus on accelerated achievement of neonatal mortality targets and 'single digit' stillbirth rates through improved home based and facility based management of sick newborns. District hospitals must ensure screening and treatment of growth related problems, birth defects, genetic diseases and provide palliative care for children. The policy affirms commitment to pre-emptive care (aimed at pre-empting the occurrence of diseases) to achieve optimum levels of child and adolescent health. The policy envisages school health programmes as a major focus area as also health and hygiene being made a part of the school curriculum. The policy gives special emphasis to the health challenges of adolescents and long term potential of investing in their health care. The scope of Reproductive and Sexual Health should be expanded to address issues like inadequate calorie intake, nutrition status and psychological problems interalia linked to misuse of technology, etc.

**4.3 Interventions to Address Malnutrition and Micronutrient Deficiencies:** Malnutrition, especially micronutrient deficiencies, restricts survival, growth and development of children. It contributes to morbidity and mortality in vulnerable population, resulting in substantial diminution in productive capacity in adulthood and consequent reduction in the nation's economic growth and well-being. Recognising this, the policy declares that micronutrient deficiencies would be addressed through a well-planned strategy on micronutrient interventions. Focus would be on reducing micronutrient malnourishment and augmenting initiatives like micro nutrient supplementation, food fortification, screening for anemia and public awareness. A systematic approach to address heterogeneity in micronutrient adequacy across regions in the country with focus on the more vulnerable sections of the population, is needed. Hence, screening for multiple micronutrient deficiencies is advocated. During the critical period of pregnancy, lactation, early childhood, adolescence and old age, the consequences of deficiencies are particularly severe and many are irreversible. While dietary diversification remains the most desirable way forward, supplementation and fortification require to be considered as short and medium term solutions to fill nutrient gaps. The present efforts of Iron Folic Acid(IFA) supplementation, calcium supplementation during pregnancy, iodized salt, Zinc and Oral Rehydration Salts/Solution(ORS), Vitamin A supplementation, needs to be intensified and increased. Sustained efforts are to be made to ensure outreach to every beneficiary, which in turn necessitates that intensive monitoring mechanisms are put in place. The policy advocates developing a strong evidence base, of the burden of collective micronutrient deficiencies, which should be correlated with disease burden and in particular for understanding the etiology of anemia. Policy recommends exploring fortified food and micronutrient sprinkles for addressing deficiencies through Anganwadi centers and

schools. Recognising the complementary role of various nutrition-sensitive interventions from different platforms, the policy calls for synergy of inputs from departments like Women and Child Development, Education, WASH, Agriculture and Food and Civil Supplies. Policy envisages that the MoHFW would take on the role of convener to monitor and ensure effective integration of both nutrition-sensitive and nutrition-specific interventions for coordinated optimal results.

- 4.4 Universal Immunization:** Priority would be to further improve immunization coverage with quality and safety, improve vaccine security as per National Vaccine Policy 2011 and introduction of newer vaccines based on epidemiological considerations. The focus will be to build upon the success of Mission Indradhanush and strengthen it.
- 4.5 Communicable Diseases:** The policy recognizes the interrelationship between communicable disease control programmes and public health system strengthening. For Integrated Disease Surveillance Programme, the policy advocates the need for districts to respond to the communicable disease priorities of their locality. This could be through network of well-equipped laboratories backed by tertiary care centers and enhanced public health capacity to collect, analyze and respond to the disease outbreaks.
- 4.5.1 Control of Tuberculosis:** The policy acknowledges HIV and TB co infection and increased incidence of drug resistant tuberculosis as key challenges in control of Tuberculosis. The policy calls for more active case detection, with a greater involvement of private sector supplemented by preventive and promotive action in the workplace and in living conditions. Access to free drugs would need to be complemented by affirmative action to ensure that the treatment is carried out, dropouts reduced and transmission of resistant strains are contained.
- 4.5.2 Control of HIV/AIDS:** While the current emphasis on prevention continues, the policy recommends focused interventions on the high risk communities (MSM, Transgender, FSW, etc.) and prioritized geographies. There is a need to support care and treatment for people living with HIV/AIDS through inclusion of 1st, 2nd and 3rd line antiretroviral (ARV), Hep-C and other costly drugs into the essential medical list.
- 4.5.3 Leprosy Elimination:** To carry out Leprosy elimination the proportion of grade-2 cases amongst new cases will become the measure of community awareness and health systems capacity, keeping in mind the global goal of reduction of grade 2 disability to less than 1 per million by 2020. Accordingly, the policy envisages proactive measures targeted towards elimination of leprosy from India by 2018.
- 4.5.4 Vector Borne Disease Control:** The policy recognizes the challenge of drug resistance in Malaria, which should be dealt with by changing treatment regimens with logistics support as appropriate. New National Programme for prevention and control of Japanese Encephalitis (JE)/Acute Encephalitis Syndrome (AES) should be accelerated with strong component of inter-sectoral collaboration.



The policy recognizes the interrelationship between communicable disease control programmes and public health system strengthening. Every one of these programmes requires a robust public health system as their core delivery strategy. At the same time, these programmes also lead to strengthening of healthcare systems.

**4.6 Non-Communicable Diseases:** The policy recognizes the need to halt and reverse the growing incidence of chronic diseases. The policy recommends to set-up a National Institute of Chronic Diseases including Trauma, to generate evidence for adopting cost effective approaches and to showcase best practices. This policy will support an integrated approach where screening for the most prevalent NCDs with secondary prevention would make a significant impact on reduction of morbidity and preventable mortality. This would be incorporated into the comprehensive primary health care network with linkages to specialist consultations and follow up at the primary level. Emphasis on medication and access for select chronic illness on a 'round the year' basis would be ensured. Screening for oral, breast and cervical cancer and for Chronic Obstructive Pulmonary Disease (COPD) will be focused in addition to hypertension and diabetes. The policy focus is also on research. It emphasizes developing protocol for mainstreaming AYUSH as an integrated medical care. This has a huge potential for effective prevention and therapy, that is safe and cost-effective. Further the policy commits itself to support programmes for prevention of blindness, deafness, oral health, endemic diseases like fluorosis and sickle cell anaemia/thalassemia, etc. The National Health Policy commits itself to culturally appropriate community centered solutions to meet the health needs of the ageing community in addition to compliance with constitutional obligations as per the Maintenance and Welfare of Parents and Senior Citizens Act, 2007. The policy recognizes the growing need for palliative and rehabilitative care for all geriatric illnesses and advocates the continuity of care across all levels. The policy recognizes the critical need of meeting the growing demand of tissue and organ transplant in the country and encourages widespread public awareness to promote voluntary donations.

**4.7 Mental Health:** This policy will take into consideration the provisions of the National Mental Health Policy 2014 with simultaneous action on the following fronts:

- Increase creation of specialists through public financing and develop special rules to give preference to those willing to work in public systems.
- Create network of community members to provide psycho-social support to strengthen mental health services at primary level facilities and
- Leverage digital technology in a context where access to qualified psychiatrists is difficult.

**4.8 Population Stabilization:** The National Health Policy recognises that improved access, education and empowerment would be the basis of successful population stabilization. The policy imperative is to move away from camp based services with all its attendant problems of quality, safety and dignity of women, to a situation where these services are available on any day of the week or at least on a

fixed day. Other policy imperatives are to increase the proportion of male sterilization from less than 5% currently, to at least 30% and if possible much higher.

5. **Women's Health & Gender Mainstreaming:** There will be enhanced provisions for reproductive morbidities and health needs of women beyond the reproductive age group (40+) This would be in addition to package of services covered in the previous paragraphs.
6. **Gender based violence (GBV):** Women's access to healthcare needs to be strengthened by making public hospitals more women friendly and ensuring that the staff have orientation to gender – sensitivity issues. This policy notes with concern the serious and wide ranging consequences of GBV and recommends that the health care to the survivors/ victims need to be provided free and with dignity in the public and private sector.
7. **Supportive Supervision:** For supportive supervision in more vulnerable districts with inadequate capacity, the policy will support innovative measures such as use of digital tools and HR strategies like using nurse trainers to support field workers.
8. **Emergency Care and Disaster Preparedness:** Better response to disasters, both natural and manmade, requires a dispersed and effective capacity for emergency management. It requires an army of community members trained as first responder for accidents and disasters. It also requires regular strengthening of their capacities in close collaboration with the local self-government and community based organisations. The policy supports development of earthquake and cyclone resistant health infrastructure in vulnerable geographies. It also supports development of mass casualty management protocols for CHC and higher facilities and emergency response protocols at all levels. To respond to disasters and emergencies, the public healthcare system needs to be adequately skilled and equipped at defined levels, so as to respond effectively during emergencies. The policy envisages creation of a unified emergency response system, linked to a dedicated universal access number, with network of emergency care that has an assured provision of life support ambulances, trauma management centers—
  - one per 30 lakh population in urban areas and
  - one for every 10 lakh population in rural areas
9. **Mainstreaming the Potential of AYUSH:** For persons who so choose, this policy ensures access to AYUSH remedies through co-location in public facilities. Yoga would be introduced much more widely in school and work places as part of promotion of good health as adopted in National AYUSH Mission (NAM). The policy recognizes the need to standardize and validate Ayurvedic medicines and establish a robust and effective quality control mechanism for AYUSH drugs. Policy recognizes the need to nurture AYUSH system of medicine, through development of infrastructural facilities of teaching institutions, improving quality control of drugs, capacity building of institutions and professionals. In addition, it recognizes the need for building research and public health skills for preventive and promotive healthcare. Linking AYUSH systems with ASHAs and VHSNCs would be an important plank of this policy. The National Health Policy would continue mainstreaming of AYUSH with general health system but with the addition of a mandatory bridge course that gives

competencies to mid-level care provider with respect to allopathic remedies. The policy further supports the integration of AYUSH systems at the level of knowledge systems, by validating processes of health care promotion and cure. The policy recognizes the need for integrated courses for Indian System of Medicine, Modern Science and Ayurgenomics. It puts focus on sensitizing practitioners of each system to the strengths of the others. Further the development of sustainable livelihood systems through involving local communities and establishing forward and backward market linkages in processing of medicinal plants will also be supported by this policy. The policy seeks to strengthen steps for farming of herbal plants. Developing mechanisms for certification of 'prior knowledge' of traditional community health care providers and engaging them in the conservation and generation of the raw materials required, as well as creating opportunities for enhancing their skills are part of this policy.

10. **Tertiary care Services:** The policy affirms that the tertiary care services are best organized along lines of regional, zonal and apex referral centers. It recommends that the Government should set up new Medical Colleges, Nursing Institutions and AIIMS in the country following this broad principle. Regional disparities in distribution of these institutions must be addressed. The policy supports periodic review and standardization of fee structure and quality of clinical training in the private sector medical colleges. The policy enunciates the core principle of societal obligation on the part of private institutions to be followed. This would include:

- Operationalization of mechanisms for referral from public health system to charitable hospitals.
- Ensuring that deserving patients can be admitted on designated free / subsidized beds.

The policy proposes to consider forms of resource generation, where corporate hospitals and medical tourism earnings are through a high degree of associated hospitality arrangements and on account of certain procedures and services, as a form of resource mobilization towards the health sector. The policy recommends establishing National Healthcare Standards Organization and to develop evidence based standard guidelines of care applicable both to public and private sector. The policy shows the way forward in developing partnership with non-government sector through empaneling the socially motivated and committed tertiary care centers into the Government efforts to close the specialist gap.

To expand public provisioning of tertiary services, the Government would additionally purchase select tertiary care services from empaneled non-government sector hospitals to assist the poor. Coverage in terms of population and services will expand gradually. The policy recognizes development of evidence based standard guidelines of care, applicable both to public and private sector as essential.

11. **Human Resources for Health:** There is a need to align decisions regarding judicious growth of professional and technical educational institutions in the health sector, better financing of professional and technical education, defining professional boundaries and skill sets, reshaping the pedagogy of

professional and technical education, revisiting entry policies into educational institutions, ensuring quality of education and regulating the system to generate the right mix of skills at the right place. This policy recommends that medical and para-medical education be integrated with the service delivery system, so that the students learn in the real environment and not just in the confines of the medical school. The key principle around the policy on human resources for health is that, workforce performance of the system would be best when we have the most appropriate person, in terms of both skills and motivation, for the right job in the right place, working within the right professional and incentive environment.

**11.1 Medical Education:** The policy recommends strengthening existing medical colleges and converting district hospitals to new medical colleges to increase number of doctors and specialists, in States with large human resource deficit. The policy recognizes the need to increase the number of post graduate seats. The policy supports expanding the number of AIIMS like centers for continuous flow of faculty for medical colleges, biomedical and clinical research. National Knowledge Network shall be used for Tele-education, Tele-CME, Tele-consultations and access to digital library. A common entrance exam is advocated on the pattern of NEET for UG entrance at All India level; a common national-level Licentiate/exit exam for all medical and nursing graduates; a regular renewal at periodic intervals with Continuing Medical Education (CME) credits accrued, are important recommendations. This policy recommends that the current pattern of MCQ (Multiple Choice Question) based entrance test for post graduates medical courses- that drive students away from practical learning- should be reviewed. The policy recognizes the need to revise the under graduate and post graduate medical curriculum keeping in view the changing needs, technology and the newer emerging disease trends. Keeping in view, the rapid expansion of medical colleges in public and private sector there is an urgent need to review existing institutional mechanisms to regulate and ensure quality of training and education being imparted. The policy recommends that the discussion on recreating a regulatory structure for health professional education be revisited to address the emerging needs and challenges.

**11.2 Attracting and Retaining Doctors in Remote Areas:** Policy proposes financial and non-financial incentives, creating medical colleges in rural areas; preference to students from under-served areas, realigning pedagogy and curriculum to suit rural health needs, mandatory rural postings, etc. Measures of compulsion- through mandatory rotational postings dovetailed with clear and transparent career progression guidelines are valuable strategies. A constant effort, therefore, needs to be made to increase the capacity of the public health systems to absorb and retain the manpower. The total sanctioned posts of doctors in the public sector should increase to ensure availability of doctors corresponding to the accepted norms. Exact package of policy measures would vary from State to State and would change over time.

**11.3 Specialist Attraction and Retention:** Proposed policy measures include - recognition of educational options linked with National Board of Examination & College of Physicians and Surgeons, creation of specialist cadre with suitable pay scale, up-gradation of short term training to medical officers to provide basic specialist services at the block and district level, performance linked payments and popularise MD (Doctor of Medicine) course in Family Medicine or General Practice. The policy recommends that the National Board of Examinations should expand the post graduate training up to

the district level. The policy recommends creation of a large number of distance and continuing education options for general practitioners in both the private and the public sectors, which would upgrade their skills to manage the large majority of cases at local level, thus avoiding unnecessary referrals.

**11.4 Mid-Level Service Providers:** For expansion of primary care from selective care to comprehensive care, complementary human resource strategy is the development of a cadre of mid-level care providers. This can be done through appropriate courses like a B.Sc. in community health and/or through competency-based bridge courses and short courses. These bridge courses could admit graduates from different clinical and paramedical backgrounds like AYUSH doctors, B.Sc. Nurses, Pharmacists, GNM, etc and equip them with skills to provide services at the sub-centre and other peripheral levels. Locale based selection, a special curriculum of training close to the place where they live and work, conditional licensing, enabling legal framework and a positive practice environment will ensure that this new cadre is preferentially available where they are needed most, i.e. in the under-served areas.

**11.5 Nursing Education:** The policy recognises the need to improve regulation and quality management of nursing education. Other measures suggested are - establishing cadres like Nurse Practitioners and Public Health Nurses to increase their availability in most needed areas. Developing specialized nursing training courses and curriculum (critical care, cardio-thoracic vascular care, neurological care, trauma care, palliative care and care of terminally ill), establishing nursing school in every large district or cluster of districts of about 20 to 30 lakh population and establishing Centers of Excellence for Nursing and Allied Health Sciences in each State. States which have adequate nursing institutions have flexibility to explore a gradual shift to three year nurses even at the sub-centre level to support the implementation of the comprehensive primary health care agenda.

**11.6 ASHA:** This policy supports certification programme for ASHAs for their preferential selection into ANM, nursing and paramedical courses. While most ASHAs will remain mainly voluntary and remunerated for time spent, those who obtain qualifications for career opportunities could be given more regular terms of engagement. Policy also supports enabling engagements with NGOs to serve as support and training institutions for ASHAs and to serve as learning laboratories on future roles of community health workers. The policy recommends revival and strengthening of Multipurpose Male Health Worker cadre, in order to effectively manage the emerging infectious and non-communicable diseases at community level. Adding a second Community Health Worker would be based on geographic considerations, disease burdens, and time required for multiple tasks to be performed by ASHA/ Community Health Worker.

**11.7 Paramedical Skills:** Training courses and curriculum for super specialty paramedical care (perfusionists, physiotherapists, occupational therapists, radiological technicians, audiologists, MRI technicians, etc.) would be developed. The policy recognises the role played by physiotherapists, occupational and allied health professionals keeping in view the demographic and disease transition the country is faced with and also recognises the need to address their shortfall. Planned expansion of allied

technical skills- radiographers, laboratory technicians, physiotherapists, pharmacists, audiologists, optometrists, occupational therapists with local employment opportunities, is a key policy direction. The policy would allow for multi-skilling with different skill sets so that when posted in more peripheral hospitals there is more efficient use of human resources.

**11.8 Public Health Management Cadre:** The policy proposes creation of Public Health Management Cadre in all States based on public health or related disciplines, as an entry criteria. The policy also advocates an appropriate career structure and recruitment policy to attract young and talented multi-disciplinary professionals. Medical & health professionals would form a major part of this, but professionals coming in from diverse backgrounds such as sociology, economics, anthropology, nursing, hospital management, communications, etc. who have since undergone public health management training would also be considered. States could decide to locate these public health managers, with medical and non-medical qualifications, into same or different cadre streams belonging to Directorates of health. Further, the policy recognizes the need to continuously nurture certain specialized skills like entomology, housekeeping, bio-medical waste management, bio medical engineering communication skills, management of call centres and even ambulance services.

**11.9 Human Resource Governance and leadership development:** The policy recognizes that human resource management is critical to health system strengthening and healthcare delivery and therefore the policy supports measures aimed at continuing medical and nursing education and on the job support to providers, especially those working in professional isolation in rural areas using digital tools and other appropriate training resources. Policy recommends development of leadership skills, strengthening human resource governance in public health system, through establishment of robust recruitment, selection, promotion and transfer postings policies.

**12. Financing of Health Care:** The policy advocates allocating major proportion (upto two-thirds or more) of resources to primary care followed by secondary and tertiary care. Inclusion of cost-benefit and cost effectiveness studies consistently in programme design and evaluation would be prioritized. This would contribute significantly to increasing efficiency of public expenditure. A robust National Health Accounts System would be operationalized to improve public sector efficiency in resource allocation/ payments. The policy calls for major reforms in financing for public facilities – where operational costs would be in the form of reimbursements for care provision and on a per capita basis for primary care. Items like infrastructure development and maintenance, non-incentive cost of the human resources i.e salaries and much of administrative costs, would however continue to flow on a fixed cost basis. Considerations of equity would be factored in- with higher unit costs for more difficult and vulnerable areas or more supply side investment in infrastructure. Total allocations would be made on the basis of differential financial ability, developmental needs and high priority districts to ensure horizontal equity through targeting specific population sub groups, geographical areas, health care services and gender related issues. A higher unit cost or some form of financial incentive payable to facilities providing a measured and certified quality of care is recommended.

**12.1 Purchasing of Healthcare Services:** The existing Government financed health insurance schemes shall be aligned to cover selected benefit package of secondary and tertiary care services purchased from public, not for profit and private sector in the same order of preference, subject to availability of quality services on time as per defined norms. The policy recommends creating a robust independent mechanism to ensure adherence to standard treatment protocols by public and non-government hospitals. In this context the policy recognizes the need of mandatory disclosure of treatment and success rates across facilities in a transparent manner. It recommends compliance to right of patients to access information about their condition and treatment. For need based purchasing of secondary and tertiary care from non-government sector, multistakeholder institutional mechanisms would be created at Centre and State levels – in the forms of trusts or registered societies with institutional autonomy. These agencies would also be charged with ensuring that purchasing is strategic - giving preference to care from public facilities where they are in a position to do so - and developing a market base through encouraging the creation of capacity in services in areas where they are needed more. Private 'not for profit' and 'for - profit' hospitals would be empanelled with preference for the former, for comparable quality and standards of care. The payments will be made by the trust/society on a reimbursement basis for services provided.

**13. Collaboration with Non-Government Sector/Engagement with private sector:** The policy suggests exploring collaboration for primary care services with 'not- for -profit' organizations having a track record of public services where critical gaps exist, as a short term measure. Collaboration can also be done for certain services where team of specialized human resources and domain specific organizational experience is required. Private providers, especially those working in rural and remote areas or with under-serviced communities, could be offered encouragement through provision of appropriate skills to meet public health goals, opportunities for skill up-gradation to serve the community better, participation in disease notification and surveillance efforts, sharing and supporting certain high value services. The policy supports voluntary service in rural and under-served areas on pro-bono basis by recognised healthcare professionals under a 'giving back to society' initiative. The policy advocates a positive and proactive engagement with the private sector for critical gap filling towards achieving National goals. One form is through engagement in public goods, where the private sector contributes to preventive or promotive services without profit- as part of CSR work or on contractual terms with the Government. The other is in areas where the private sector is encouraged to invest- which implies an adequate return on investment i.e on commercial terms which may entail contracting, strategic purchasing, etc. The policy advocates for contracting of private sector in the following activities:

**13.1 Capacity building:** Outsourcing of training of teachers to strengthen school health programmes by adopting neighbourhood schools for quarterly training modules.

**13.2 Skill Development programmes:** Recognising that there are huge gaps in technicians, nursing and para- nursing, para-medical staff and medical skills in select areas, the policy advocates coordination between National Council for Skill Development, MOHFW and State Government(s) for engaging private hospitals/private general medical practitioners in skill development.

- 13.3 Corporate Social Responsibility (CSR):** CSR is an important area which should be leveraged for filling health infrastructure gaps in public health facilities across the country. The private sector could use the CSR platform to play an active role in the awareness generation through campaigns on occupational health, blood disorders, adolescent health, safe health practices and accident prevention, micronutrient adequacy, anti-microbial resistance, screening of children and ante-natal mothers, psychological problems linked to misuse of technology, etc. The policy recommends engagement of private sector through adoption of neighbourhood schools/ colonies/ slums/tribal areas/backward areas for healthcare awareness and services.
- 13.4 Mental healthcare programmes-** Training community members to provide psychological support to strengthen mental health services in the country. Collaboration with Government would be an important plank to develop a sustainable network for community/locality towards mental health.
- 13.5 Disaster Management** is another area where collaboration with private sector would enable better outcomes especially in the areas of medical relief and post trauma counselling/treatment. A pool of human resources from private sector could be generated to act as responders during disasters. The private sector could also pool their infrastructure for quick deployment during disasters and emergencies and help in creation of a unified emergency response system. Additionally sharing information on infrastructure and services deployable for disaster management would enable development of a comprehensive information system with data on availability and utilization of services, for optimum use during golden hour and other emergencies.
- 13.6 Strategic Purchasing as Stewardship:** Directing areas for investment for the commercial health sector.
- 13.6.1** The health policy recognizes that there are many critical gaps in public health services which would be filled by "strategic purchasing". Such strategic purchasing would play a stewardship role in directing private investment towards those areas and those services for which currently there are no providers or few providers. The policy advocates building synergy with "not for profit" organisations and private sector subject to availability of timely quality services as per predefined norms in the collaborating organisation for critical gap filling.
- 13.6.2** The main mechanisms of strategic purchasing are insurance and through trusts. Schemes like Arogyasri and RSBY have been able to increase private participation significantly. Payment is by reimbursement on a fee for service basis and many private providers have been able to benefit greatly by these schemes. The aim would be to improve health outcomes and reduce out of pocket payments while minimising moral hazards and - so that these schemes can be scaled up and made more effective. The policy provides for preferential treatment to collaborating private hospitals/institutes for CGHS empanelment and in proposed strategic purchase by Government subject to other requirements being met.
- 13.6.3** For achieving the objective of having fully functional primary healthcare facilities- especially in urban areas to reach under-served populations and on a fee basis for middle class populations, Government would collaborate with the private sector for operationalizing such health and wellness



centres to provide a larger package of comprehensive primary health care across the country. Partnerships that address specific gaps in public services: These would inter alia include diagnostics services, ambulance services, safe blood services, rehabilitative services, palliative services, mental healthcare, telemedicine services, managing of rare and orphan diseases.

- 13.6.4** The policy advocates building synergy with “not for profit” organisations and private sector subject to availability of timely quality services as per predefined norms in the collaborating organisation for critical gaps.
- 13.7 Enhancing accessibility in private sector:** The policy recommends a better public private healthcare interface and recognizes the need for engagement in operationalization of mechanisms for referrals from public health system. Charitable hospitals and “not for profit” hospitals may volunteer for accepting referrals from public health facilities. The private sector could also provide for increased designated free/ subsidized beds in their hospitals for the downtrodden, poor and others towards societal cause.
- 13.8 Role in Immunization:** The policy recognizes the role of the private sector in immunization programmes and advocates their continued collaboration in rendering immunization service as per protocol.
- 13.9 Disease Surveillance:** Towards strengthening disease surveillance, the private sector laboratories could be engaged for data pooling and sharing. All clinical establishments would be encouraged to notify diseases and provide information of public health importance.
- 13.10 Tissue and organ transplantations:** Tissue and organ transplantations and voluntary donations are areas where private sector provides services- but it needs public interventions and support for getting organ donations. Recognising the need for awareness, the private sector and public sector could play a vital role in awareness generation.
- 13.11 Make in India:** Towards furthering “Make in India”, the private domestic manufacturing firms/ industry could be engaged to provide customized indigenous medical devices to the health sector and in creation of forward and backward linkages for medical device production. The policy also seeks assured purchase by Government health facilities from domestic manufacturers, subject to quality standards being met.
- 13.12 Health Information System:** The objective of an integrated health information system necessitates private sector participation in developing and linking systems into a common network/grid which can be accessed by both public and private healthcare providers. Collaboration with private sector consistent with Meta Data and Data Standards and Electronic Health Records would lead to developing a seamless health information system. The private sector could help in creation of registries of patients and in documenting diseases and health events.
- 13.13 Incentivising Private Sector :** To encourage participation of private sector, the policy advocates incentivizing the private sector through inter alia (i) reimbursement/ fees (ii) preferential treatment to collaborating private hospitals/institutes for CGHS empanelment and in proposed strategic

purchase by Government, subject to other requirements being met (iii) Non-financial incentives like recognition/ acknowledgement/ felicitation and skill upgradation to the private sector hospitals/practitioners for providing public health services and for partnering with the Government of India/State Governments in health care delivery and (iv) through preferential purchase by Government health facilities from domestic manufacturers, subject to quality standards being met.

- 13.14** Private sector engagement goes beyond contracting and purchasing. Private providers, especially those working in rural and remote areas, or with under-serviced communities, require access to opportunities for skill up-gradation to meet public health goals, to serve the community better, for participation in disease notification and surveillance efforts, and for sharing and support through provision of certain high value services- like laboratory support for identification of drug resistant tuberculosis or other infections, supply of some restricted medicines needed for special situations, building flexibilities into standards needed for service provision in difficult contexts and even social recognition of their work. This would greatly encourage such providers to do better. Hitherto all public training and skill provision has been only to public providers. The policy recognises the need for training and skilling of many small private providers and recommends the same.
- 14. Regulatory Framework:** The regulatory role of the Ministry of Health and Family Welfare- which includes regulation of clinical establishments, professional and technical education, food safety, medical technologies, medical products, clinical trials, research and implementation of other health related laws-needs urgent and concrete steps towards reform. This will entail moving towards a more effective, rational, transparent and consistent regime.
- 14.1 Professional Education Regulation:** The policy calls for a major reform in this area. It advocates strengthening of six professional councils (Medical, Ayurveda Unani & Siddha, Homeopathy, Nursing, Dental and Pharmacy) through expanding membership of these councils between three key stakeholders - doctors, patients and society in balanced numbers. The policy supports setting up of National Allied Professional Council to regulate and streamline all allied health professionals and ensure quality standards.
- 14.2 Regulation of Clinical Establishments:** A few States have adopted the Clinical Establishments Act 2010. Advocacy with the other States would be made for adoption of the Act. Grading of clinical establishments and active promotion and adoption of standard treatment guidelines would be one starting point. Protection of patient rights in clinical establishments (such as rights to information, access to medical records and reports, informed consent, second opinion, confidentiality and privacy) as key process standards, would be an important step. Policy recommends the setting up of a separate, empowered medical tribunal for speedy resolution to address disputes /complaints regarding standards of care, prices of services, negligence and unfair practices. Standard Regulatory framework for laboratories and imaging centers, specialized emerging services such as assisted reproductive techniques, surrogacy, stem cell banking, organ and tissue transplantation and Nano Medicine will be created as appropriate.

**14.3 Food Safety:** The policy recommends putting in place and strengthening necessary network of offices, laboratories, e-governance structures and human resources needed for the enforcement of Food Safety and Standards (FSS) Act, 2006.

**14.4 Drug Regulation:** Prices and availability of drugs are regulated by the Department of Pharmaceuticals. However, with regard to other areas of drugs and pharmaceuticals, this policy encourages the streamlining of the system of procurement of drugs; a strong and transparent drug purchase policy for bulk procurement of drugs; and facilitating spread of low cost pharmacy chain such as Jan Aushadhi stores linked with ensuring prescription of generic medicines. It further recommends education of public with regard to branded and non-branded generic drugs. The setting up of common infrastructure for development of the pharmaceutical industry will also be promoted. The policy advocates strengthening and rationalizing the drug regulatory system, promotion of research and development in the pharmaceutical sector and building synergy and evolving a convergent approach with related sectors.

**14.5 Medical Devices Regulation:** The policy recommends strengthening regulation of medical devices and establishing a regulatory body for medical devices to unleash innovation and the entrepreneurial spirit for manufacture of medical device in India. The policy supports harmonization of domestic regulatory standards with international standards. Building capacities in line with international practices in our regulatory personnel and institutions, would have the highest priority. Post market surveillance program for drugs, blood products and medical devices shall be strengthened to ensure high degree of reliability and to prevent adverse outcomes due to low quality and/or refurbished devices/health products.

**14.6 Clinical Trial Regulation:** Clinical trials are essential for new product discovery and development. With the objective of ensuring the rights, safety and well-being of clinical trial participants, while facilitating such trials as are essential, specific clause(s) be included in the Drugs and Cosmetics Act for its regulation. Transparent and objective procedures shall be specified, and functioning of ethics and review committees will be strengthened. The Global Good Clinical Practice Guidelines, which specifies standards, roles and responsibilities of sponsors, investigators and participants would be adhered to. Irrational drug combination will continue to be monitored and controlled and appropriate regulatory framework for standardization of AUSH drugs will be ensured. Clear and transparent guidelines, with independent monitoring mechanisms, are the ways forward to foster a progressive and innovative research environment, while safeguarding the rights and health of the trial participants.

**14.7 Pricing- Drugs, Medical Devices and Equipment:** The regulatory environment around pricing requires a balance between the patients concern for affordability and industry's concern for adequate returns on investment for growth and sustainability. Timely revision of National List of Essential Medicines (NLEM) along with appropriate price control mechanisms for generic drugs shall remain a key strategy for decreasing costs of care for all those patients seeking care in the private sector. An approach on the same lines but suiting specific requirements of the sectors would be considered for price control with regard to a list of essential diagnostics and equipment.

- 15 **Vaccine Safety:** Vaccine safety and security would require effective regulation, research and development for manufacturing new vaccines in accordance with National Vaccine Policy 2011. The policy advocates commissioning more research and development for manufacturing new vaccines, including against locally prevalent diseases. It recommends building more public sector manufacturing units to generate healthy competition; uninterrupted supply of quality vaccines, developing innovative financing and creating assured supply mechanisms with built in flexibility. Units such as the integrated vaccine complex at Chengalpattu would be set up and vaccine, anti-sera manufacturing units in the public sector upgraded with increase in their installed capacity.
- 16 **Medical Technologies:** India is known as the pharmacy of the developing world. However, its role in new drug discovery and drug innovations including bio-pharmaceuticals and bio-similars for its own health priorities is limited. This needs to be addressed in the context of progress towards universal health care. Making available good quality, free essential and generic drugs and diagnostics, at public health care facilities is the most effective way for achieving the goal. The free drugs and diagnostics basket would include all that is needed for comprehensive primary care, including care for chronic illnesses, in the assured set of services. At the tertiary care level too, at least for in-patients and out-patients in geriatric and chronic care segments, most drugs and diagnostics should be free or subsidized with fair price selling mechanisms for most and some co-payments for the "well-to-do".
17. **Public Procurement:** Quality of public procurement and logistics is a major challenge to ensuring access to free drugs and diagnostics through public facilities. An essential pre-requisite that is needed to address the challenge of providing free drugs through public sector, is a well-developed public procurement system.
18. **Availability of Drugs and Medical Devices:** The policy accords special focus on production of Active Pharmaceutical Ingredient (API) which is the back-bone of the generic formulations industry. Recognizing that over 70% of the medical devices and equipments are imported in India, the policy advocates the need to incentivize local manufacturing to provide customized indigenous products for Indian population in the long run. The goal with respect to medical devices shall be to encourage domestic production in consonance with the "Make in India" national agenda. Medical technology and medical devices have a multiplier effect in the costing of healthcare delivery. The policy recognizes the need to regulate the use of medical devices so as to ensure safety and quality compliance as per the standard norms.
19. **Aligning other policies for medical devices and equipment with public health goals:** For medical devices and equipment, the policy recommends and prioritises establishing sufficient labeling and packaging requirements on part of industry, adequate medical devices testing facility and effective port - clearance mechanisms for medical products.
20. **Improving Public Sector Capacity for Manufacturing Essential Drugs and Vaccines:** Public sector capacity in manufacture of certain essential drugs and vaccines is also essential in the long term for the health security of the country and to address some needs which are not attractive commercial

propositions. These public institutions need more investment, appropriate HR policies and governance initiatives to enable them to become comparable with their benchmarks in the developed world.

- 21. Anti-microbial resistance:** The problem of anti-microbial resistance calls for a rapid standardization of guidelines, regarding antibiotic use, limiting the use of antibiotics as Over-the-Counter medication, banning or restricting the use of antibiotics as growth promoters in animal livestock. Pharmacovigilance including prescription audit inclusive of antibiotic usage, in the hospital and community, is a must in order to enforce change in existing practices.
- 22. Health Technology Assessment:** Health Technology assessment is required to ensure that technology choice is participatory and is guided by considerations of scientific evidence, safety, consideration on cost effectiveness and social values. The National Health Policy commits to the development of institutional framework and capacity for Health Technology Assessment and adoption.
- 23. Digital Health Technology Eco - System:** Recognising the integral role of technology (eHealth, mHealth, Cloud, Internet of things, wearables, etc) in the healthcare delivery, a National Digital Health Authority (NDHA) will be set up to regulate, develop and deploy digital health across the continuum of care. The policy advocates extensive deployment of digital tools for improving the efficiency and outcome of the healthcare system. The policy aims at an integrated health information system which serves the needs of all stake-holders and improves efficiency, transparency, and citizen experience. Delivery of better health outcomes in terms of access, quality, affordability, lowering of disease burden and efficient monitoring of health entitlements to citizens, is the goal. Establishing federated national health information architecture, to roll-out and link systems across public and private health providers at State and national levels consistent with Metadata and Data Standards (MDDS) & Electronic Health Record (EHR), will be supported by this policy. The policy suggests exploring the use of "Aadhaar" (Unique ID) for identification. Creation of registries (i.e. patients, provider, service, diseases, document and event) for enhanced public health/big data analytics, creation of health information exchange platform and national health information network, use of National Optical Fibre Network, use of smartphones/tablets for capturing real time data, are key strategies of the National Health Information Architecture.
- 23.1 Application of Digital Health:** The policy advocates scaling of various initiatives in the area of tele-consultation which will entail linking tertiary care institutions (medical colleges) to District and Sub-district hospitals which provide secondary care facilities, for the purpose of specialist consultations. The policy will promote utilization of National Knowledge Network for Tele-education, Tele-CME, Tele-consultations and access to digital library.
- 23.2 Leveraging Digital Tools for AYUSH:** Digital tools would be used for generation and sharing of information about AYUSH services and AYUSH practitioners, for traditional community level healthcare providers and for household level preventive, promotive and curative practices.
- 24. Health Surveys:** The scope of health, demographic and epidemiological surveys would be extended to capture information regarding costs of care, financial protection and evidence based policy planning and reforms. The policy recommends rapid programme appraisals and periodic disease specific surveys



to monitor the impact of public health and disease interventions using digital tools for epidemiological surveys.

**25. Health Research:** The National Health Policy recognizes the key role that health research plays in the development of a nation's health. In knowledge based sector like health, where advances happen daily, it is important to increase investment in health research.

**25.1 Strengthening Knowledge for Health:** The policy envisages strengthening the publicly funded health research institutes under the Department of Health Research, the apex public health institutions under the Department of Health & Family Welfare, as well as those in the Government and private medical colleges. The policy supports strengthening health research in India in the following fronts- health systems and services research, medical product innovation (including point of care diagnostics and related technologies and internet of things) and fundamental research in all areas relevant to health- such as Physiology, Biochemistry, Pharmacology, Microbiology, Pathology, Molecular Sciences and Cell Sciences. Policy aims to promote innovation, discovery and translational research on drugs in AUSH and allocate adequate funds towards it. Research on social determinants of health along with neglected health issues such as disability and transgender health will be promoted. For drug and devices discovery and innovation, both from Allopathy and traditional medicines systems would be supported. Creation of a Common Sector Innovation Council for the Health Ministry that brings together various regulatory bodies for drug research, the Department of Pharmaceuticals, the Department of Biotechnology, the Department of Industrial Policy and Promotion, the Department of Science and Technology, etc. would be desirable. Innovative strategies of public financing and careful leveraging of public procurement can help generate the sort of innovations that are required for Indian public health priorities. Drug research on critical diseases such as TB, HIV/AIDS, and Malaria may be incentivized, to address them on priority. For making full use of all research capacity in the nation, grant- in- aid mechanisms which provide extramural funding to research efforts is envisaged to be scaled up.

**25.2 Drug Innovation & Discovery:** Government policy would be to both stimulate innovation and new drug discovery as required, to meet health needs as well as ensure that new drugs discovered and brought into the market are affordable to those who need them most. Similar policies are required for discovering more affordable, more frugal and appropriate point of care diagnostics as also robust medical equipment for use in our rural and remote areas. Public procurement policies and public investment in priority research areas with greater coordination and convergence between drug research institutions, drug manufacturers and premier medical institutions must also be aligned to drug discovery.

**25.3 Development of Information Databases:** There is also a need to develop information data-bases on a wide variety of areas that researchers can share. This includes ensuring that all unit data of major publicly funded surveys related to health, are available in public domain in a research friendly format.

**25.4 Research Collaboration:** The policy on international health and health diplomacy should leverage India's strength in cost effective innovations in the areas of pharmaceuticals, medical devices, health care delivery and information technology. Additionally leveraging international cooperation, especially

involving nations of the Global South, to build domestic institutional capacity in green-field innovation and for knowledge and skill generation could be explored.

## 26. Governance

**26.1 Role of Centre & State:** One of the most important strengths and at the same time challenges of governance in health is the distribution of responsibility and accountability between the Centre and the States. The policy recommends equity sensitive resource allocation, strengthening institutional mechanisms for consultative decision-making and coordinated implementation, as the way forward. Besides, better management of fiduciary risks, provision of capacity building, technical assistance to States to develop State-specific strategic plans, through the active involvement of local self-government and through community based monitoring of health outputs is also recommended. The policy suggests State Directorates to be strengthened by HR policies, central to which is the issue that those from a public health management cadre must hold senior positions in public health.

**26.2 Role of Panchayati Raj Institutions:** Panchayati Raj Institutions would be strengthened to play an enhanced role at different levels for health governance, including the social determinants of health. There is need to make Community Based Monitoring and Planning (CBMP) mandatory, so as to place people at the centre of the health system and development process for effective monitoring of quality of services and for better accountability in management and delivery of health care services.

**26.3 Improving Accountability:** The policy would be to increase both horizontal and vertical accountability of the health system by providing a greater role and participation of local bodies and encouraging community monitoring, programme evaluations along with ensuring grievance redressal systems.

## 27. Legal Framework for Health Care and Health Pathway

One of the fundamental policy questions being raised in recent years is whether to pass a health rights bill making health a fundamental right- in the way that was done for education. The policy question is whether we have reached the level of economic and health systems development so as to make this a justiciable right- implying that its denial is an offense. Questions that need to be addressed are manifold, namely, (a) whether when health care is a State subject, is it desirable or useful to make a Central law, (b) whether such a law should mainly focus on the enforcement of public health standards on water, sanitation, food safety, air pollution etc, or whether it should focus on health rights- access to health care and quality of health care – i.e whether focus should be on what the State enforces on citizens or on what the citizen demands of the State? Right to healthcare covers a wide canvas, encompassing issues of preventive, curative, rehabilitative and palliative healthcare across rural and urban areas, infrastructure availability, health human resource availability, as also issues extending beyond health sector into the domain of poverty, equity, literacy, sanitation, nutrition, drinking water availability, etc. Excellent health care system needs to be in place to ensure effective implementation of the health rights at the grassroots level. Right to health cannot be perceived unless the basic health infrastructure like doctor-patient ratio, patient-bed ratio, nurses-patient ratio, etc are near or above threshold levels and uniformly spread-out across the geographical frontiers of the country. Further, the procedural

guidelines, common regulatory platform for public and private sector, standard treatment protocols, etc need to be put in place. Accordingly, the management, administrative and overall governance structure in the health system needs to be overhauled. Additionally, the responsibilities and liabilities of the providers, insurers, clients, regulators and Government in administering the right to health need to be clearly spelt out. The policy while supporting the need for moving in the direction of a rights based approach to healthcare is conscious of the fact that threshold levels of finances and infrastructure is a precondition for an enabling environment, to ensure that the poorest of the poor stand to gain the maximum and are not embroiled in legalities. The policy therefore advocates a progressively incremental assurance based approach, with assured funding to create an enabling environment for realizing health care as a right in the future.

## **28. Implementation Framework and Way Forward**

A policy is only as good as its implementation. The National Health Policy envisages that an implementation framework be put in place to deliver on these policy commitments. Such an implementation framework would provide a roadmap with clear deliverables and milestones to achieve the goals of the policy.



Department of Health and Family Welfare  
(e-Health Division)

\*\*\*

**Subject: Minutes of review/consultation meeting held on 24.03.2017  
regarding Electronic Health Care Data Privacy & Security**

A meeting was held under the chairmanship of AS&DG(CGHS), MoHFW on 24<sup>th</sup> March 2017 in Room No. 153 A at 10.30 Nirman Bhawan to review/consult on the latest draft (Version 3.0) of the **Electronic Health Care Data Privacy & Security Act** prepared by National Law School of India University (NLSIU). The list of participants is provided at Annexure I.

2. AS&DG(CGHS) welcomed the participants and briefed about the agenda of the meeting. He then requested the participants to present their views/suggestions on the latest draft Act (which was circulated in advance) for consideration by NLSIU while working further on the draft.

3. NLSIU representative mentioned that the 'Substantive Part' of the draft Act is regarding:

- Confidentiality, privacy, ownership of electronic health care data
- Issue of standardization, storage & transmission of data
- Establishment of National eHealth Authority (NeHA), its roles & power
- Nature of punishment (civil or criminal) etc., for data breach
- Setting up of Adjudicating Authority & Appellate Tribunal

Further they briefed the changes made w.r.t. the previous draft version V2.0.

4. After detailed discussion in the meeting, the following key suggestions were made by the participants on select items/clauses, which were duly noted by NLSIU for due consideration/incorporation so as the draft could be further fine-tuned before finalisation.

- a. It was discussed that the current draft has some sections where technical aspects are described in details. It was suggested that such sections would be extracted and will be placed separately in rules and guidelines section. In addition sections related to Health Information Exchange may not require so much of detailing and may be put under Rules.
- b. During deliberations it came out that there are several operational & technical clauses/details mentioned in the draft, which may be put under Rules
- c. It was suggested that NeHA may be given "quasi-judicial" status and accordingly be assigned powers.
- d. For giving right to the patient to choose destruction of his/her data, it was suggested that this function may be left with the National eHealth Authority which may deliberate on this issue and decide whether to give patient any rights regarding destruction of the patient data.
- e. Some of the terms mentioned in the act such as 'sensitive electronic healthcare data' require more detailed elaboration in the definitions sections.

- f. It was suggested that secretariat for NeHA need not be mentioned in the Act.
  - g. Minor editing corrections were suggested in few sections which were noted by NLSIU.
  - h. It was also suggested that the title and presentation outline of the draft Act be modified in such a way to be named & presented as "National Digital Health Authority (NDHA) Act" encompassing mandate for "establishment of NDHA, rather than NeHA with roles, responsibilities, power, organisation set-up etc. and setting up of Appellate Tribunal". National Health Policy 2017 mentions about setting up of National Digital Health Authority (NDHA).
5. In the meeting it was **decided** that a sub-committee drawing members from Ministry, Industry and other stakeholder group(s), as appropriate, be constituted so as to hold discussion & work closely with NLSIU for inputs, modification and finalisation of the draft Act, which could then be put in public domain for inviting comments/suggestions.
6. **in the meeting, it was also decided that the revised Draft after appropriately incorporating the modifications/inputs as suggested by the participants may be placed in public domain, after due approval of Hon'ble HFM, for seeking comments/suggestions.**

The meeting ended with vote of thanks to the Chairman.

#### Annexure I:

1. Dr R K Vats, AS&DG, MoHFW- Chairman
2. Shri Sunil Sharma, JS (eHealth)
3. Shri Rajendra Pratap Gupta, Advisor to HFM
4. Dr O V Nandimath, Registrar, NLSIU
5. Shri Prashant Desai, Expert Committee Member, NLSIU
6. Shri Viay Thakur, Director, MeitY
7. Shri Anirudh Sen, Deputy Director, FICCI
8. Prof S N Sarbadhikari, PD, CHI of NHP, NIHFW
9. Dr B S Bedi, Advisor, C-DAC, Pune
10. Shri Gaur Sunder, Joint Director, C-DAC, Pune
11. Prof Narsh Gipta, Director-Professor, MAMC and Associated Hospital
12. Shri Arvind Sivaramakrishnan, CIO, Apollo Hospitals
13. Dr Milind Antani, Legal and Tax Counselling Worldwide, Nishith Desai Associates,
14. Shri S B Bhattacharya, Head Health Informatics, TCS

D/ 3023 836/2016

स्पीड पोस्ट द्वारा  
BY SPEED POSTसाधारण डेली डेली  
BY ORDINARY POST

File No. Q-11013/6/2015-eGov

Government of India / भारत सरकार



Ministry of Health and Family Welfare/ स्वास्थ्य एवं परिवार कल्याण विभाग

e-Governance Section / (ई गवर्नेंस अनुभाग)

\*\*\*\*\*

by speed Post

Nirman Bhawan, New Delhi

Dated 11 February, 2016

To

Prof. (Dr) O.V Nandimath, Registrar,  
National Law School of India University  
P.O Bag 7201, Nagarbhavi  
Bangalore 560072, Karnataka.

**Subject:** Awarding the work of drafting of Legislation on Electronic Health Data Privacy, Confidentiality and Security in India.

Dear Sir,

This is with reference to the financial proposal submitted by National Law School of India University (NLSIU), Nagarbhavi, Bangalore to Ministry of Health and Family Welfare (MoHFW) for drafting of Legislation on Electronic Health Data Privacy, Confidentiality and Security in India.

- It is informed that MoHFW has agreed to engage NLSIU, Bangalore for drafting the work of Legislation on Electronic Health Data Privacy, Confidentiality and Security in India.
- You're requested to kindly confirm the acceptance of the work and provide the MoU and invoice for the advance payment of the fees latest by 25<sup>th</sup> February, 2016.

(Jitendra Arora)

Director (eGovernance)

Ministry of Health &amp; Family Welfare

Phn: 23062317

o/c

**NATIONAL LAW SCHOOL OF INDIA UNIVERSITY**  
**NAGARBHAVI, BANGALORE-560 242**

(114)

**Commercial Proposal for**  
**Drafting the Proposed Legislation for Electronic Health Data Privacy & Security**

Sl. No.	Particulars	Amount
1	Ice-breaking Consultation	300,000.00
2	Principal Investigator & Co-ordinator (Rs.60,000 x 12 months)	720,000.00
3	Advisory Board (meeting, honorarium etc. (Rs.50,000 x 4 meetings)	200,000.00
4	Team Members	
	a. Drafting Specialist (Rs.30,000 x 12 months)	360,000.00
	b. Research Assistant (Health Law) (Rs.15,000 x 12 m)	180,000.00
	c. Research Assistant (Human Rights) (Rs.15,000 x 12 m)	180,000.00
5	Administrative Expenses (Travel, Books, Reference Material, Photocopying, Printing & communication etc.)	250,000.00
6	Secretarial Assistance (Rs.5,000 x 12 months)	60,000.00
	Sub total	2,250,000.00
7	Institutional Charges @ 20% of the total sum	450,000.00
	Total	2,700,000.00

14.1.2016  
 FINANCE OFFICER  
 National Law School of India University  
 BANGALORE - 72

**Note:-**

- 1 Only the Ice-breaking consultation is factored into the budget
- 2 Primary consultation and wider consultation- As the cost involved in this regard is not assessable right now, they are not included. However, the proposal is (a) NLSIU will incur the initial cost and the same will be reimbursed by MoH&FA; or (b) the consultations are organized by MoH&FW itself
- 3 The Financial proposal will have a validity of 90 days
- 4 70% of the total amount to be released immediately after the acceptance (with award letter); 30% within 15 days after submission of the 'Final Draft'
- 5 The applicable service tax is in addition to the above indicated quote
- 6 The MoH&FW will nominate one of its senior officer to act as Nodal Officer, to whom the communications are to be sent and anything communicated to the Nodal Officer is deemed to be communicated to MoH&FW
- 7 The total duration of the project, as per the agreement between the parties (at Delhi, after the presentation on 1st December, 2015 will be 12 months
- 8 Subject to 7 above, other details of our earlier proposal/presentation stand and would determine the basic scope of work
- 9 Principal Investigator & Co-ordinator will have the discretion to inter allocate/shuffle the resource allocation to churn out the quality work, without exceeding the final quote.



## MEMORANDUM OF UNDERSTANDING FOR CONSULTANCY SERVICES

**THIS MEMORANDUM OF AGREEMENT FOR CONSULTANCY** (hereinafter referred to as MoU or Agreement as the case may be, unless context deserves otherwise) on the day of 15<sup>th</sup> February, 2016 is executed between

The e-Governance Division, **Department of Health and Family Welfare, Ministry of Health & Family Welfare (MoH&FW), Government of India, Nirman Bhawan, New Delhi- 110011** on the **FIRST PART**

**AND**

The **National Law School of India University** (hereinafter referred to as NLSIU or Consultant as the context deserves), a University established under the National Law School of India Act, 1987 (Karnataka Act 22 of 1986), the maiden university sponsored by the Bar Council of India, the professional regulatory body in India, on the **SECOND PART**

**WHEREAS** the e-Governance Division, Department of Health and Family Welfare under Ministry of Health and Family Welfare, Government of India is desirous to have a comprehensive Legislation on "Electronic Health Data Privacy, Confidentiality and Security in India" and selected NLSIU for the said job through a competitive process.

**WHEREAS** the e-Governance Division, Department of Health and Family Welfare under Ministry of Health and Family Welfare, Government of India,



realizes the need to hire the expertise of NLSIU in getting the law drafted; which will be the culmination of their policy reform efforts in the respective area.

**FURTHER WHEREAS** the said object and outcome Parties agree as follows:

1. The entire drafting of the Electronic Health Data Privacy, Confidentiality and Security in India is generally envisaged to be carried out in four stages, comprising of the following
  - a. **First Stage** – initial meeting between both the Parties to the agreement at Delhi or any such other mutually agreeable place;
  - b. **Second Stage** – Maiden Consultation with 'experts' in the field, preferably at NLSIU or such other mutually convenient place;
  - c. **Third Stage** – primary and wider consultations with experts in respective fields and other stakeholders, if necessary; and
  - d. **Fourth Stage** – actual drafting work to be carried out by NLSIU on the lines of 'Background Note' provided by the First Party.

**EXPLANATION:** Without prejudice to anything contained in this MoU and agreement between the Parties, the stages mentioned above are tentative and Parties, are at liberty to change the course suitably, keeping in mind the overall objective of the project.

2. **THE EFFECTIVE DATE** – The effective date shall be the date on which both the Parties sign this MoU, or else the date on which last party signs the MoU, as the case may be.

3. **METHODOLOGY**–

- a. The First Party will forward relevant literature as required, which shall include – policy /consultation papers on the same subject and such other related subjects or areas, the approach paper, background note(prepared by e-Governance Division, MoH&FW) etc., to NLSIU, Bangalore immediately after the Effective Date; but earlier to the 'initial meeting' between the Parties, unless otherwise different strategy in this regard is mutually agreed between the Parties.
- b. In case, there is any further requirement of any other relevant documents from e-Governance Division, MoH&FW, it may be requested by NLSIU; and the same will be made available to it within reasonable period of time, preferably not exceeding 15 days from the date of request.
- c. **INITIAL MEETING** – After the study of the existing legislations/regulations/Acts on Data Privacy & Security in India and other select countries, an 'Initial Meeting' will be held with the senior executives (including members from the relevant Committees notified) of the First Party at New Delhi, or any such mutually agreed place. During this phase of meetings, NLSIU will understand the

*off*

'context' and theoretical basis of the drafting; any other relevant issues to be effectively addressed in the draft legislation.

- d. During this meeting parties may by mutual agreement, fine-tune and finalise the table of contents as endorsed by Legal Sub-group under EHR Standards Committee of MoH&FW.
- e. **DRAFTING OF LEGISLATION ON ELECTRONIC HEALTH DATA PRIVACY, CONFIDENTIALITY AND SECURITY**– This forms the central part of the consultancy. NLSIU will start drafting of the law, by taking assistance of such expert personnel and experts in the field. The drafting will be completed within the stipulated period and the 'First Draft of the Electronic Health Data Privacy, Confidentiality and Security Act' will be submitted.
- f. **SUBMISSION OF DRAFT BILL** – The first draft Act as per the time line (as per Clause 5 of this MoU) will be submitted for the perusal and consideration of the First Party. The First Party may suggest modifications, amendments, changes etc., to the submitted draft Act, as necessary and all such suggestions will be taken into account and the first draft will be revised and the final draft report will be submitted.
- g. Along with the submission of draft bill NLSIU may also submit all relevant background and explanatory notes which are required to understand the choice of formulation made. The exact process of consultation documents as well as background notes would be mutually agreed between the Nodal Officers.





**4. SUBMISSION OF FINAL (DRAFT) BILL**

- a. The First Party will submit the Final Act to Ministry of Health and Family Welfare, Government of India to seek approval after incorporating all the suggestions/ modifications suggested by the MoH&FW on the draft Act.
- b. One hardcopy and soft copy (in CD drive) of the report including 'final draft bill' will then be submitted to the First Party.
- c. After receipt of the final report the First Party shall acknowledge the receipt of the Report; and that shall also be taken as conclusion of the consultancy engagement between the parties.

**5. DURATION OF THE CONSULTANCY**

- a. The total duration of the consultancy is agreed to be seven (7) calendar months to be calculated from signing of MoU to the submission of the 'Final Draft Bill', with the following mile stones:
  - (i) The submission of First Draft report to The Department of Health and Family Welfare (e-Governance Section) – six (06) months from the effective date.
  - (ii) Submission of Final draft – maximum of one (01) month from the date of submission of the First draft.
- b. Notwithstanding the above expression in (a) Parties are at liberty to extend the time by mutual agreement with no added financial commitments.

6. **THE EXPECTED OUTCOME** – considering the creative nature of the consultancy, parties understand the draft on 'Electronic Health Data Privacy, Confidentiality and Security Act' along with 'Statement of Objectives', documents and explanatory notes specified in clause 3(g) of this MoU will be the outcome of this consultancy.
7. NLSIU shall constitute as far as possible the team; however, it retains the autonomy in selecting the team, subject to producing the quality output as per the requirements of MoH&FW.
8. **RESPONSIBILITIES OF THE PARTIES** – Within 10 days from the effective date each Party shall communicate to other:
- a) The First Party shall communicate the nomination of the Nodal Officer on its behalf and his coordinates to the Second Party;
  - b) The Second Party shall communicate the selection of the Principal Investigator (who will also be the Nodal Officer of NLSIU) and his coordinates to the First Party;
  - c) Such Nodal Officer shall be the single contact point between the Parties; any notice or communication to such a Nodal Officer shall be deemed as notice or communication passed on to the respective Party and shall be binding on that Party.
  - d) The respective Nodal Officers shall communicate to each other all the developments periodically.

- e) Both the Parties shall provide all such relevant information to facilitate the drafting of the said law.

**9. PRICE FOR CONSULTANCY etc.,**

- a. Total price of the consultancy is agreed between the parties as INR 27,00,000.00 (Rupees Twenty Seven Lakhs only) which shall include necessary institutional charges, excluding applicable service taxes,;
- b. Except Maiden Consultation any other consultation shall be charged separately;
- c. Any other additional expenses shall be borne by the First Party;
- d. Following is the payment break-up procedure, agreed by the parties
- (i) 40% of the total amount to be paid immediately from the effective date;
  - (ii) 30% of the total amount to be paid within 3 months from the effective date
  - (iii) 30% of the total amount to be paid within 15 days after submission of the 'Final Draft'.
- e. Notwithstanding anything stated in this MoU, NLSIU has factored the travel cost for its members for the 'Maiden Consultation', which can be held at Delhi or such other mutually convenient place. Any additional consultation or consultations, other than NLSIU consulting the experts on their own, shall be borne by MoH&FW on cost or reimbursement basis, as the case may be.



- f. NLSIU will specify the bank account details to The Department of Health and Family Welfare (e-Governance Section), MoH&FW, Government of India, New Delhi to electronically transfer the money; alternatively, the instrument of price may be transferred by a Demand Draft drawn in favour of 'National Law School of India University, Bangalore'.
- g. NLSIU will submit copies of valid PAN card and Service Tax Registration Certificate of the institution (if any) to The Department of Health and Family Welfare (e-Governance Section), MoH&FW, Government of India, New Delhi, before release of 1<sup>st</sup> instalment/release of funds.

#### 10. CONFIDENTIALITY

- a. NLSIU shall treat all documents/data/information or part of them, which is provided to them, as strictly confidential and maintain secrecy for the same.
- b. NLSIU shall not publish, disclose any information about, make available or otherwise dispose of the documents/data/information or any part or parts thereof to any third party, directly or indirectly without prior written consent of the e-Governance Division, Department of Health and Family Welfare, MoH&FW, Government of India, New Delhi.
- c. NLSIU shall restrict access to the documents/data/information only to those of its employees to whom it will be felt necessary and relevant for this project and shall draw the provision of this undertaking to the



personal attention of those of its employees to whom access to the document/data/information will be granted.

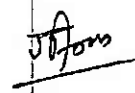
11. **TERMINATION FOR DEFAULT**– either of the parties to this MoU, without notice prejudice to any relevant remedy for breach of contract, by written notice of 15 days, sent to other, may terminate this MoU either in whole or in part.

12. **DISPUTE RESOLUTION** – In case of any grievance or disputes, the Parties shall resolve disputes through mutual negotiations.

13. All earlier proposals, commercials and communications shall remain unchanged.

(for NLSIU)

(for e-Governance Division, MoH&FW)

**PROF.(DR.) R. VENKATA RAO**

**SHRI. JITENDRA ARORA**

Vice-Chancellor, NLSIU

Director, e-Governance Division, MoH&FW


**WITNESSES:**

1.

(NANDIMATH - O.V)

2.

(A. SANYAL)  
 Secretary  
 Ministry of Health & F.W.  
 भारत सरकार/Govt. of India  
 नई दिल्ली/New Delhi

9 | Page

(जीतिन्द्र अरोड़ा)  
 (JITENDRA ARORA)  
 निदेशक/Director  
 स्वास्थ्य एवं परिवार कल्याण विभाग  
 Ministry of Health & F.W.  
 भारत सरकार/Govt. of India  
 नई दिल्ली/New Delhi

### **Brief Note on National Digital Health Authority of India Act**

There are a variety of reasons for placing a high value on protecting the privacy, confidentiality, and security of health information. Some theorists depict privacy as a basic human good or right with intrinsic value. They see privacy as being objectively valuable in itself, as an essential component of human well-being. They believe that respecting privacy (and autonomy) is a form of recognition of the attributes that give humans their moral uniqueness.

The more common view is that privacy is valuable because it facilitates or promotes other fundamental values, including ideals of personhood such as:

- 1) Personal autonomy (the ability to make personal decisions)
- 2) Individuality
- 3) Respect
- 4) Dignity and worth as human beings

The bioethics principle nonmaleficence<sup>1</sup> requires safeguarding personal privacy. Breaches of privacy and confidentiality not only may affect a person's dignity, but can cause harm. When personally identifiable health information, for example, is disclosed to an employer, insurer, or family member; it can result in stigma, embarrassment, and discrimination. Thus, without some assurance of privacy, people may be reluctant to provide candid and complete disclosures of sensitive information even to their physicians. Ensuring privacy can promote more effective communication between physician and patient, which is essential for quality of care, enhanced autonomy, and preventing economic harm, embarrassment, and discrimination. However, it should also be noted that perceptions of privacy vary among individuals and various groups. Data that are considered intensely private by one person may not be by others.

Privacy can foster socially beneficial activities like health research. Individuals are more likely to participate in and support research if they believe their privacy is being protected. Protecting privacy is also seen by some as enhancing data quality for research and quality improvement initiatives. When individuals avoid health care or engage in other privacy-protective behaviours, such as withholding information, inaccurate and incomplete data are entered into the health care system. These data, which are subsequently used for research, public health reporting, and outcomes analysis, carry with them the same vulnerabilities.

The bioethics principle of respect for persons also places importance on individual autonomy, which allows individuals to make decisions for themselves, free from coercion, about matters that are important to their own well-being. Indian society also places a high value on individual autonomy, and one way to respect persons and enhance individual autonomy is to ensure that people can make the choice about when, and whether, personal information (particularly sensitive information) can be shared with others.

There are a number of Health Systems currently implemented which collect health/clinical data of patients/citizens on a large scale. As a result huge health/clinical data repositories are being created. This requires adequate rules and regulations and institutional mechanism to address Privacy & security related challenges/concerns.

---

<sup>1</sup> The ethical principle of doing no harm, based on the Hippocratic maxim, primum non nocere, first do no harm.

In India there are different legislations specific to particular health conditions/circumstances including mental/physical illness, disability, communicable diseases etc. key legislations/regulations in Health domain and their salient features pertaining to privacy/confidentiality are briefed subsequently. These include:

- A. Medical Council of India's Code of Ethics Regulations, 2002
- B. Epidemics Diseases Act, 1897
- C. Mental Health Act, 1987
- D. The Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995
- E. Pre-Natal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994
- F. Medical Termination of Pregnancy Act, 1971
- G. Insurance Regulatory and Development Authority (Third Party Administrators) Health Services Regulations, 2001
- H. Ethical Guidelines for Biomedical Research on Human Subjects.

The Information Technology Act, 2000 provides legal recognition to any transaction, which is done by electronic way or use of Internet. The issue of data protection has been addressed in Information Technology Amendment Act, 2008. It protects private information that is obtained by agencies by virtue of powers conferred under the Act.

The existing legislations in health domain cover some aspects of privacy & security specific only to the mandated/limited scope. The IT Act, providing legal recognition to any transaction done by electronic way or use of Internet, covers issue of personal data protection, collected for specific purpose of electronic transaction. The key aspects which have been observed lacking under the existing legislations generally include consent, collection & purpose limitation, access & correction, penalty/offences/liability & remedy, security etc.

The need for statute specifically covering data privacy & security aspects in a comprehensive manner in Health Sector emerges more imperative in the context of promotion & adoption of e-Health on a large scale through establishment of pan-India Integrated Health Information System and EHR System including setting up of Health Information Exchanges under Digital India Programme.

The prime objective of National Digital Health Authority of India Act is to establish National Digital Health Authority and Health Information Exchanges and to provide for effective digital health care data privacy, confidentiality, security and standardization. This Act shall apply to all digital medical records, digital health records or digital personal/protected health data. This Act shall supersede other existing laws with respect to digital medical record, digital health record or digital personal/protected health information or digital health care data.

National Digital Health Authority of India is an institutional mechanism established by the Central Government to encourage standardization, integration and exchange of digital health information amongst the various healthcare providers and recognizing that the

digital collection, storage, processing and transmission of personal health data requires adhering to the highest standard of data protection by prescribing norms for collection, storage, transmission and disclosure of digital health care data by NDHAI. NDHAI shall act as licensing authority to establish Health Information Exchange by prescribing standards and norms. The Central Government prescribe rules for the implementation of this law.

National Digital Health Authority of India Act provides for establishment of Adjudicating Authority/ies by the Central Government by notifying under this Act, depending upon the local requirements. The Central Government by notifying under this Act, shall also establish an Appellate Tribunal to hear appeals against the orders of the Adjudicating Authority/ies. Any person aggrieved by any decision or order of the Appellate tribunal can file an appeal to the High Court.

National Digital Health Authority of India Act prescribes sanctions for the breach of digital health care data. The authorities established under this Act shall follow the procedure prescribed by Civil Procedure Code and Criminal Procedure Code in adjudicating the disputes.



F.No Z-18015/10/2013-eGov  
Government of India  
Ministry of Health & Family Welfare  
(e-Governance Division)

\*\*\*

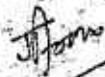
New Delhi, dated the 20<sup>th</sup> April, 2015

NOTICE

**Subject:** Placing the Concept Note on National e-Health Authority (NeHA) on public domain for comments/views-reg.

It is informed that the last date for submission of comments/views on the Concept Note on National e-Health Authority (NeHA) has been extended to 10<sup>th</sup> May 2015.

The comments/views may be forwarded to Director (e-Governance), Ministry of Health and Family Welfare, Room No 307-D, Nirman Bhawan, New Delhi-110108 or emailed at [jitendra.arora@gov.in](mailto:jitendra.arora@gov.in) on or before 10<sup>th</sup> May, 2015.



(Jitendra Arora)

Director(e-Governance Division)

Phn No. 23062317

F.No Z-18015/10/2013-eGov  
Government of India  
Ministry of Health & Family Welfare  
(e-Governance Division)

\*\*\*

New Delhi, dated the 16<sup>th</sup> March, 2015

**NOTICE**

**Subject:** Placing the Concept Note on National e-Health Authority (NeHA) on public domain for comments/views-reg.

Ministry of Health and Family Welfare proposes to set up a National e-Health Authority (NeHA) responsible for development of an Integrated Health Information System in India. It will also be responsible for enforcing the laws & regulations relating to the privacy and security of the patients health information & records. Accordingly, a Concept Note on establishment of NeHA has been placed in public domain with a view to elicit comments/views of the stakeholders including the general public.

The comments/views may be forwarded to Director (e-Governance Division), Ministry of Health and Family Welfare, Room No 307-D, Nirman Bhawan, New Delhi-110108 or emailed at [jitendra.arora@gov.in](mailto:jitendra.arora@gov.in) on or before 20<sup>th</sup> April, 2015.



(Jitendra Arora)  
Director(e-Governance Division)  
Phn No. 23062317

## National eHealth Authority (NeHA)

### Executive Summary

This note brings out relevance and importance of the proposed National eHealth Authority (NeHA) as a promotional, regulatory and standards setting organization to guide and support India's journey in e-Health and consequent realization of benefits of ICT intervention in Health sector in an orderly way. It also spells out the proposed functions and governance mechanism of NeHA. These draw from earlier recommendations of high level bodies in India as also global experience.

It is also strongly recommended that NeHA be created at the earliest, as it will give a fillip to all the current and envisaged programs of the government in respect of IT in Health and accelerated adoption of EHR in an orderly manner. It will also help avoid problems arising out of uncoordinated induction of IT systems in hospitals and public health systems which will become inevitable with the passage of time in the absence of a suitable authority to guide and enforce orderly evolution.

## 1. Background

### 1.1 Indian Health Care System

The Indian health care system is one of India's largest and most complex sectors. It delivers services to a diverse population of approximately 1.24 billion across a wide range of geographic and socioeconomic settings. Services are provided by a complex network of public and private care providers, ranging from a single doctor rural PHCs (Primary Health Centres) to specialty and super-specialty health care institutions like the medical college hospitals in the public sector and from a single doctor

outpatient clinic to large trust or corporate hospitals and third party providers in the private sector.

India spends around 4.1% of GDP on health, of which only about 1.1% is the contribution of the government. Out of pocket expenses are high at over 60%, much higher than most of the countries in the world. Given that India today enjoys a demographic dividend which can contribute to the productivity and prosperity of the nation, the healthcare system is specially and fundamentally important to the country from both an economic and social perspective. A health population underpins strong economic growth, community well-being and prosperity.

#### India's disease burden

Due to the size of the population, high percentage of rural population (32% urban versus 68% rural) with rapidly growing urbanization, industrialization, environmental degradation and the persisting inequality in health status between and within States/UTs, India currently faces a "Triple burden of diseases", namely:

1. Unfinished agenda of Communicable Diseases
2. Emerging Non-Communicable Diseases related to lifestyles and
3. Emerging Infectious Diseases

Life expectancy at birth stands at 66 (both sexes), Infant mortality rate at 43.8, Under-5 mortality rate at 56 (both per 1000 live births), Maternal mortality ratio at 190 (per 100,000 live births), Total fertility rate at 2.5 and Adult Mortality rate (probability of dying between 15 and 60 years per 1000 population) at 242/160 (m/f). Prevalence of HIV has come down to 169, Incidence of Malaria to 1523 and Tuberculosis to 230 – all per 100,000 of population. In terms of mortality, (% of total deaths, all ages, both sexes), deaths due to communicable, maternal, perinatal and nutritional conditions account for 28%, Injuries 12% and Non-Communicable Deaths (NCDs) account for 60% (with a distribution of Cardiovascular diseases

26%, Cancers 7%, Chronic respiratory diseases 13%, Diabetes 2% and other NCDs 12%).

WHO Disease and Injury Country estimates indicate that 22,750 to 29,500 life-years are lost in India out of 100,000 life-years due to any cause; of this NCDs account for 43% of the DALYs (Disability-Adjusted Life Year).

In terms of utilization of health services, Contraceptive prevalence was at 55%, Antenatal care (4+ visits) at 50%, Birth attended by skilled health personnel at 67%, Measles immunization (1-yr olds) at 74% and Smear-positive TB treatment-success at 88%.

However, adult risk factors remain high on account of Tobacco use (aged 15+) for males at 25% (2011), Raised blood pressure (aged 25+) at 23.1 (2008) and Raised blood glucose (aged 25+) at 11.1 (2008). Further, while percentage of population using improved water has risen to ~95%, the situation remains poor in respect of using improved sanitation at less than 40%.

Against the above challenges, Indian healthcare system suffers from acute shortage of physicians and quality paramedics; per 10,000 population, doctors are at 7 and Nurses and midwives at 17.1, much below WHO recommended numbers. The situation is much worse in rural areas. Technology can play an enabling role in addressing the issue of absence of qualified service delivery personnel in remote areas, in improving the efficiency of the healthcare system and also in improving the quality of care.

This will require a fundamental shift in the way information is accessed and shared across the health system. We have to move away from a reliance on tools such as pen, paper and human memory to an environment where beneficiaries, providers and health care managers / administrators can reliably and securely access and share health information in real time across geographic and health sector boundaries.

The only way this can be achieved is through the implementation of world class ICT interventions and adoption of e-Health.

### 1.2 Use of ICT in the Indian Healthcare System

One of the major challenges faced by a patient in India today is that, whenever he visits any healthcare provider he is examined, typically undergoes a certain number of tests and the care provider initiates a treatment plan for his/her condition. If there is a subsequent need to visit another healthcare provider either within the same care setting or, as is more often than not, a different one, he/she is likely to undergo the same process of repeating examination, testing and treatment unless and until he carries around his medical records diligently irrespective of its size or form.

Over a period, many of the public and private hospitals have developed their own healthcare systems or hospital information systems that have served patients well, but without a focus on standards adoption, or the interoperability aspect and interconnection of systems across hospital settings that can lead to continuity of care – leading to ineffective results. Such non-interoperable discrete islands of information have created significant barriers to the effective sharing of information between healthcare participants, an issue compounded by India's multiple health service boundaries and geographic distances. It also poses real challenges when trying to understand and report what is really happening in the Indian healthcare system to support population health surveillance and guide policy, service planning, innovation and clinician and operational decision making.

With vendors incorporating different standards for similar or same systems, it is little wonder that inefficiency, waste and errors in healthcare

information and delivery management are all too commonplace an occurrence. Consequently, a patient's health information often gets trapped in silos of legacy systems, unable to be shared with members of the healthcare community.

### 1.3 Complexities associated with the present eHealth system

Current eHealth IT systems in India are riddled with multiple complexities, largely arising out of compartmentalized approach to development of the ecosystem by various stakeholders, as opposed to a coordinated or integrated approach. The consequences of these include: Legacy systems, silos of data and multiple incompatible standards (arising partly out of lack of national standards until recently for IT and health informatics as well as those for reporting, identity and the like); poor or modest penetration of Hospital Information Systems; lack of demand and regulation for integration or exchange of EHRs across providers; challenges from vendors in terms of support to integration and easy to use interfaces; lack of focus on patient services and patient engagement; non-availability of Minimum Data Sets (MDS) and EHRs; and shortage of funding for sustainability – to name a few.

For building an interconnected e-Health system across public and private hospitals within a state or nationally, it is imperative that they should have consistent standards for identity management, data entry, messaging, data encryption, retrieval, reporting etc.

Doctors and other service providers will have to adjust their work flow in order to incorporate EHR use, and also to use the information gained for continuous improvement of their health care delivery. They may not also

be organized in a standardized / systematic way - either in the way they report / analyze the data but need to do so progressively.

To encourage standardization, integration and exchange of electronic information amongst the various healthcare providers and recognizing that the electronic collection, storage, processing and transmission of personal health data requires adherence to the highest standard of data protection, the "EMR/EHR Standards for India" were formulated after extensive discussion with all the stake holders and thereafter notified by the Government of India in September, 2013. India has also become a member of International Health Terminology Standards Development Organisation (IHTSDO) since April, 2014 to support affordable and consistent use of vocabularies through Systematized Nomenclature of Medicine Clinical terms (SNOMED-CT) by all care providers.

What is required at this stage is an institutional mechanism to guide early adoption of the EHR and SNOMED-CT standards by all care-providers as independent and continued deployment of a lot of non-conformant systems by public and private healthcare providers in states and centre can lead to an avoidable and costly situation from which putting together national e-Health system can be extremely cumbersome, time-consuming and expensive, as the experience of many countries has demonstrated.

#### 1.4 Benefits of Electronic Health Record (EHR)

EHR and the ability to exchange health information electronically can help the providers to extend higher quality and safer care for patients while creating tangible enhancements in the efficiency of operations of their organization. EHRs helps providers to: better manage care for patients by providing accurate, up-to-date, and complete information about patients at



## Concept Note- National eHealth Authority (NeHA)

the point of care; access patient records quickly for more coordinated, efficient care; share electronic information securely with patients and other clinicians; diagnose patients more effectively, reduce medical errors and provide safer care; prescribe more reliably and safer; promote legible, complete documentation and accurate, streamlined coding and billing; improve productivity and work-life balance; and reduce costs through decreased paperwork, improved safety, reduced duplication of testing, and improved health.

Critical issues in implementing EHR include: the need to streamline the processes and workflows relating to administrative and clinical functions; the need to build capacities of providers and management in introduction, operation, management and use of Hospital Information Systems meaningfully by support to various administrative and clinical functions through standards compliant EMR/EHR; the need to handle change management issues arising out of the above; and the need to ensure compliance to security, privacy and confidentiality as prescribed in standards and guidelines so that legal, audit guidelines are met and citizen and provider interests are protected.

Given constraints of resources, there are compelling benefits, outcomes and impacts of e-Health that India can ill-afford to forego in improving healthcare delivery to citizens. Notable among them include:

- a. Improved timeliness (better quality of healthcare delivery)
- b. Effectiveness (right intervention / audit trails for adverse events)
- c. Efficiency (less resources in terms of manpower, time and cost)
- d. Informed patients and their caregivers
- e. Better access

Additional and specific benefits of e-Health include: diagnostic accuracy, reduced waiting times, better referral management and greater satisfaction with services.

Given the growing penetration of mobile phones and Internet, including smartphones and tablets, other services that can be delivered on a large scale include: SMS-based services, live and asynchronous telemedicine, and interactive voice response service (IVRS).

### 1.5 International Experience

Roll-out of national e-Health systems, interconnecting EHR with unique identifiers for citizens and providers has been progressively undertaken by various countries.

Canada was one of the earliest to start in 2002, setting up Canada Health Infoway as a federally funded, independent, not-for-profit organization to lead the development and implementation of electronic health projects across Canada. It has been working with provinces and territories to invest in electronic health projects to support safer, more efficient healthcare delivery. It targets to respect patient confidentiality fully and provide private and secure systems to healthcare professionals with immediate access to complete and accurate patient information, enabling better decisions about diagnosis and treatment. Government of Canada provides supporting funding and sets national priorities through Canada Health Infoway. In many ways, it has been a pioneer in nationwide EHR system and standards.

U.K., Australia and Singapore have been other prominent countries who have taken initiatives for setting up nationwide e-Health since then.

In U.K., NHS is the provider of healthcare services for all and is funded through general taxation. Department of Health is responsible for national plans. National Program for IT (NPfIT) has been put in place to provide the information infrastructure. After some early hiccups, U.K. has

progressed in terms of creating NHS Care Records Service (NHS CRS) to improve the sharing of records of consenting patients across the NHS, providing patients access to their own records, providing a system for electronic transmission of prescriptions, creating a Picture Archiving and Communication System, ensuring a secure broadband network infrastructure to connect all NHS bodies in England, making it easier and faster for GPs and other primary care staff to book hospital appointments for patients and the like. NHS Information Centre is an independent NHS Special Health Authority that collects analyses and distributes national statistics on health and social care. It therefore has a key role in defining NHS data standards.

In Australia, National e-Health Transition Authority (NEHTA) is a not-for-profit company set up by Federal, State and Territory governments to develop better ways of electronically collecting and securely exchanging health information. NEHTA is in a unique position to influence key e-Health policy and regulation. It supports Australian healthcare system by improving the quality of healthcare services, by enabling authorized clinicians to access a patient's integrated healthcare information and history, directly sourced from clinical notes, test results and prescriptions using standardized clinical data formats and terminologies; streamlining multi-disciplinary care management, enabling seamless handovers of care by ensuring efficient electronic referrals; improving clinical and administrative efficiency, by standardizing certain types of healthcare information to be recorded in e-Health systems; maintaining high standards of patient privacy and information security and the like.

In Singapore, the National e-Policy to promote the use of ICT across all sectors has been extremely effective, as has been the public funding for ICT support of programs addressing national health priorities. Regulations to protect the privacy and security of individual patient data where e-Health is used are rated as very effective. Four Singapore public hospitals

had been awarded the Stage 6 benchmark of U.S. Healthcare Information and Management Systems Society (HIMSS) for adopting EHR systems among the very first implementations in Asia. Singapore has progressed from hospital department systems to integrated electronic orders processing, on-line radiology imaging, closed loop medication management, timely laboratory receivables and analysis results and ultimately facilitating good clinical decision support and data integration.

In United States of America, Office of National Coordinator for Health Information Technology (ONC) was created in 2004 but with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, it has been charged with building an interoperable, private and secure nationwide health information system and supporting the widespread and meaningful use of health information technology. ONC is a staff division of the Office of the Secretary within the U.S. Department of Health and Human Services. ONC leads national health IT efforts, charged as the principal federal entity to coordinate nationwide efforts to implement and use the most advanced health IT and the electronic exchange of health information.

HITECH act seeks to improve American healthcare through an unprecedented investment in health information technology. They are specifically designed to work together to provide the necessary assistance and technical support to providers, enable coordination and alignment within and among states, establish connectivity to the public health community in case of emergencies and ensure that the workforce is properly trained and equipped to be meaningful users of EHRs. The Act sets meaningful use of interoperable EHR adoption in the healthcare system as a critical national goal and incentivize EHR adoption. ONC works to improve Adoption, Standards, Incentive, Privacy and security and Governance. The Federal Health IT Strategic Plan 2011-'15 has set the goals for use of health IT as: adoption and information exchange through

## Concept Note- National eHealth Authority (NeHA)

meaningful use; improving care, improve public health and reduce healthcare costs; inspire confidence and trust in use of health IT; empower individuals to improve their health and healthcare system; and achieve rapid learning and technological advancement.

There are over thirty other countries who are building up valuable experiences in nationwide e-Health adoption, though none has truly completed the full scale adoption. ITU included adoption of e-Health as a strategic priority from 2008 onwards.

#### 1.6 Background for setting up NeHA

The National Knowledge Commission (NKC) had recommended in 2008 formation of National Health Information Authority (NHIA) to support implementation on e-Health. High Level Expert Group (HLEG) set up by Planning Commission in the context of XII Plan had recommended EHR adoption and setting up of a nationwide network to support the same. They had done so as part of recommending Universal Health Coverage.

'Digital India' Program has been announced by Government of India in August 2014 and a set of on-line Healthcare services are scheduled to be offered as part of the same in a definite time-frame in the next 4-5 years.

## 2. National eHealth Authority (NeHA)

### 2.1 Mission

NeHA will be the nodal authority that will be responsible for development of an Integrated Health Information System (including Telemedicine and mHealth) in India, while collaborating with all the stakeholders, viz., healthcare providers, consumers, healthcare technology industries, and policymakers. It will also be responsible for enforcing the laws & regulations relating to the privacy and security of the patients health information & records.

### 2.2 Vision / Goals

- a) To guide the adoption of e-Health solutions at various levels and areas in the country in a manner that meaningful aggregation of health and governance data and storage/exchange of electronic health records happens at various levels in a cost-effective manner
- b) To facilitate integration of multiple health IT systems through health information exchanges
- c) To oversee orderly evolution of state-wide and nationwide Electronic Health Record Store/Exchange System that ensures that security, confidentiality and privacy of patient data is maintained and continuity of care is ensured.

### 2.3 In the light of the above, National e-Health Authority (NeHA) has been envisaged to support:

- a) Formulation of policies, strategies and implementation plan blue-print (National eHealth Policy / Strategy) for coordinated eHealth adoption

in the country by all players; regulation and accelerated adoption of e-health in the country by public and private care providers and other players in the ecosystem; to establish a network of different institutions to promote eHealth and Tele-medicine/remote healthcare/virtual healthcare and such other measures;

- b) Formulation and management of all health informatics standards for India; Laying down data management, privacy & security policies, standards and guidelines in accordance with statutory provisions; and
- c) To promote setting up of state health records repositories and health information exchanges (HIEs);
- d) To deal with privacy and confidentiality aspects of Electronic Health Records (EHR).

#### 2.4 Functions of National eHealth Authority

##### 2.4.1 Core Functions

###### a. Policy and Promotion

- i. Working out vision, strategy and adoption plans, with timeframes, priorities and road-map in respect of eHealth adoption by all stakeholders, both Public and Private providers, formulate policies for eHealth adoption that are best suited to Indian context and enable accelerated health outcomes in terms of access, affordability, quality and reduction in disease mortality & morbidity
- ii. To engage with stakeholders through various means so that eHealth plans are adopted and other policy, regulatory and legal provisions are implemented by both the public & private sector stakeholders.
- iii. It shall provide thought leadership, in the areas of eHealth and mHealth.

b. Standards Development

- i. Government of India, MoHFW has published EMR/EHR standards for India in 2013. Similarly, MoHFW has become a member of IHTSDO with a view of widespread adoption of SNOMED-CT in India; MoHFW has also nominated C-DAC (Pune) as interim NRC (iNRC). As such, initial focus of NeHA would be on addressing implementation issues and promoting mechanisms in support of the same.
- ii. Concurrently, NeHA will be nurtured to undertake the role of a standards development, maintenance and support agency in the area of Health Informatics

c. Legal Aspects including Regulation

- i. NeHA will be setup through an appropriate legislation (Act of Parliament). It is also proposed to address the issues relating to privacy & confidentiality of Patients' EHR in the legislation. NeHA may act as an enforcement agency with suitable mandate and powers.
- ii. NeHA will be responsible for enforcement of standards & ensuring security, confidentiality and privacy of patient's health information & records.

d. Setting up and Maintaining Health Repositories, Electronic Health Exchanges and National Health Information Network

NeHA, while avoiding the implementation role by itself, will prepare documents relating to architecture, standards, policies and guidelines for e-Health stores, HIEs and NHIN; it may also initiate or encourage PoCs, in close consultation with government – centre and states, industry, implementers and users. Later, it would lay down operational guidelines



## Concept Note- National eHealth Authority (NeHA)

and protocols, policies for sharing and exchange of data, audit guidelines and the like; these shall be guided by experience in operation and use of PoC, global best practices and consultations with stake-holders (MoHFW, State governments and other public and private providers, academia, R&D labs, and others).

e. Capacity Building

Spreading awareness on Health Informatics / eHealth to healthcare delivery professionals through various educational initiatives and flexible courses according to the background of the learners will form a component of NeHA activities, as it is seen as critical to acceleration of adoption of eHealth.

f. Other functions may be assigned to NeHA as the situation warrants.

## 2.5 Governance

The Authority will have a Chairman and four full time members. The tentative composition of NeHA may be as follows:

- a) Chairman: An eminent person in the field of Medicine, Public Health or Judiciary
- b) Three full time Members: They shall be from the following fields:-  
Medicine, Public Health, IT Standards, Health Economics/Management, Administration/ Finance, Legal
- c) Member Secretary: Same as above but shall also discharge the role of co-ordination and effective functioning of the Authority.

Standing Consultative Committee: The Committee shall be chaired by Chairman of NeHA and, besides its four members, shall have members who represent experts and stake-holder community.

## Concept Note- National eHealth Authority (NeHA)

Indicative membership positions of Standing Consultative Committee are:

*Ministry of Health & Family Welfare (4) {AS&DG(CGHS), AS&MD(NHM), DGHS, Mission Leader of Health MMP}, Principal Secretaries (Health)/ Mission Leaders from States(3), Expert Doctors by rotation (2), Private Healthcare providers by rotation (2), IT industry reps by rotation (2), Standards org rep (2), DeitY rep (1), DOT rep. (1), Independent Medical Practitioners by rotation (1), MCI Chairman or nominee (1), NASSCOM & NATHEALTH Presidents (2), FICCI President, ICMR DG or nominee (1), IRDA Chairman (1), Consumer Rights Activists (2 by rotation), WHO rep (1).*

It shall meet once in six months or more often when considered necessary. It shall function as a two-way consultation forum between NeHA and diverse stake-holders to enable evolution of sound eHealth policies and road-map and solicit participation of all stake-holders in adoption of nationwide eHealth and Standards at various levels, in a manner that ensures benefits are realized in a phased and orderly manner that protects the interests of citizens/patients and providers.

The Authority will have powers to co-opt additional members to contribute to specialist needs and points of view. They shall be part-time members and will not have voting powers. Otherwise, they will have full authority to participate in all proceedings of the Authority. These members shall be co-opted on a one-year at a time basis to enable rotation of members and thus diversity of views to be heard.

### Conclusion

Health being a state subject in India and much depends on the ability / regulatory framework enacted by the State governments, NeHA shall be created through legislation (Act of Parliament) that empowers it to take leadership and strategic role for setting directions for public and private eHealth initiatives, including electronic health records storage and health information exchange capabilities and other related health information technology efforts & regulation of the same.

NeHA shall ensure ongoing interagency cooperation – while engaging with various stakeholders through the Standing Consultative Committee and also through other means, in a structured, open and transparent manner to support successful evolution of national integrated health information system.

---

### References

1. NKC report  
[http://knowledgecommission.gov.in/downloads/documents/wg\\_health.pdf](http://knowledgecommission.gov.in/downloads/documents/wg_health.pdf)
2. HLEG recommendations  
[http://planningcommission.nic.in/reports/genrep/rep\\_uhc0812.pdf](http://planningcommission.nic.in/reports/genrep/rep_uhc0812.pdf)
3. EHR Standards for India <http://mohfw.nic.in/showfile.php?lid=1672>
4. Health MMP DPR
5. Sarbadhikari SN, The State of Medical Informatics in India: A Roadmap for optimal organization, *J. Medical Systems*, 2005, 29: 125-141.
6. Integrated Health Information Architecture – Power to the Users, Design, Development and Use, Jorn Braa and Sundeep Sahay, Matrix Publications, 2012
7. Electronic Health Record, Standards, Coding Systems, Frameworks and Infrastructures, Pradeep K Sinha, Gaur Sunder et al., IEEE Press, John Wiley Press, 2013
8. IT Act, 2008  
[http://deity.gov.in/sites/upload\\_files/dit/files/downloads/itact2000/it\\_amendment\\_act2008.pdf](http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf)
9. CCA, DeitY <http://cca.gov.in/cca/index.php>
10. STQC, DeitY [www.stqc.gov.in/](http://www.stqc.gov.in/)
11. TRAI act [www.trai.gov.in/](http://www.trai.gov.in/)
12. IRDA act <https://www.irda.gov.in/>
13. Clinical Establishment Act  
<http://clinicalestablishments.nic.in/WriteReadData/386.pdf>
14. Electronic Delivery of Services Act  
[http://egovreach.in/uploads/presentation/kohima/Electronic\\_Service\\_Delivery.pdf](http://egovreach.in/uploads/presentation/kohima/Electronic_Service_Delivery.pdf)
15. Open Standards for e-Governance, DeitY  
<http://www.nic.in/services/e-Governance%20Standards>

16. IFeG, DeitY <https://egovstandards.gov.in/public-review-document/gazette-notification-technical-standards-ifeg-india>
  17. HIPAA act, 2009, U.S.A.  
[http://en.wikipedia.org/wiki/Health\\_Insurance\\_Portability\\_and\\_Accountability\\_Act](http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act)
  18. Australia e-Health Authority, <http://www.nehta.gov.au/>
  19. Canada <https://www.infoway-inforoute.ca/index.php/about-infoway>
  20. U.S. <http://www.healthit.gov/sites/default/files/oncdatabrief16.pdf>
  21. U.K. <http://www.ehi.co.uk/news/ehi/8564/nhs-england-to-publish-it-strategy>
  22. Singapore  
[https://www.moh.gov.sg/content/moh\\_web/home/Publications/educational\\_resources/2011/NationalElectronicHealthRecord.html](https://www.moh.gov.sg/content/moh_web/home/Publications/educational_resources/2011/NationalElectronicHealthRecord.html)
  23. OECD Organizational Practices in Health, Strengthening-Health-Information-Infrastructure\_Preliminary-version\_2April2013
  24. ITU on e-Health <http://www.itu.int/en/ITU-T/studygroups/2013-2016/16/Pages/ehealth.aspx>
  25. WHO on e-Health <http://www.who.int/topics/ehealth/en/>
  26. Source: <http://www.who.int/bulletin/volumes/90/5/11-099069/en/>
  27. Source: [www.ehealth-impact.org](http://www.ehealth-impact.org)
-

Minutes of the National consultation  
on setting up of  
National eHealth Authority (NeHA)  
held on 04th April, 2016

*Ministry of Health & Family Welfare (MoHFW),  
Government of India*

Place: AIIMS Board Room, New Delhi

Time: 10:00 A.M.

**National Consultation on National eHealth Authority (NeHA)****Held on 4th April, 2016****Minutes of Consultation**

A National Consultation regarding setting up of *National eHealth Authority (NeHA)* was held under the chairmanship of Secretary, Ministry of Health & Family Welfare (MoHFW) and co-chaired by **Secretary (DeitY)** on 4<sup>th</sup> April, 2016 at AIIMS, New Delhi as per agenda given in **Annexure 1**. Senior Officers from MoHFW, DeitY and representatives from more than 23 States attended the consultation. Representatives of various other organisations from health sector such as World Health Organisation (WHO), Association Bodies (IMA, FICCI, NATHEALTH and NASSCOM), private healthcare providers and healthcare IT vendors and healthcare IT experts participated in the consultation. List of the participants is provided at **Annexure – 2**.

1. **Shri Sunil Sharma, Joint Secretary (eGov), MoHFW** welcomed the participants and briefed about the Vision and Goals of **National eHealth Authority (NeHA)**. NeHA is proposed to be set up to specify standards, regulate adoption of standards/data privacy & security measures and also promote IT initiatives in health domain. One of the key roles for NeHA would be to establish eHealth systems enabling inter-operability of data across hospitals, health facilities, public health IT systems (centre & states) etc. He mentioned that there is a need to encourage EHR creation across the country along with a unique code in order to maintain online medical record for each person. He highlighted that there are over 30 countries who are taking initiatives encompassing robust laws and implementation & support structures for establishment of standards compliant EHR Systems. He further mentioned that the EHR Standards 2013 are being revised and suggestions have been invited from healthcare stakeholders.
2. **Shri Bhanu Pratap Sharma, Secretary (HFW)** suggested to leverage the use of cloud by hosting different modules of health IT systems such as Hospital Information System on cloud and mentioned that work in this regard is already underway. He informed that work for setting up an integrated health information platform is underway and as precursor to this platform, a test bed for interoperability between different health & hospital IT systems is being created which is expected to be ready for demonstration by June 2016. He also said that by this year end, an EHR standards compliant HIS would be ready for public health sector. He further mentioned that NeHA would look into the overall policy and roadmap focusing on how IT (including mobile technology) can be optimally utilized in Healthcare sector and how to leverage and integrate the existing large scale public health IT systems like Mother & Child Tracking System (MCTS) and Health Management Information System (HMIS).
3. **Dr. Aruna Sharma, Secretary (DeitY)** emphasized on the setting up of a controlling body to direct hospitals & other healthcare providers across the country to maintain their patient's health records in standardized electronic format. She also said that appropriate IT

management systems needed to be developed and put in place which could take care of the relevant concerns of patients. She said that DeitY is willing to support the MoHFW in all possible ways for achieving the goal of Digital Health.

4. **Shri K.B. Agarwal, AS (eGov), MoHFW**, mentioned regarding the critical need for unique identifiers for both patients and healthcare providers for achieving interoperability between IT systems. Aadhaar number is a suitable solution for use as patients unique identifiers. He further mentioned that a National Identification Number (NIN) process has been started wherein all health facilities both public and private would be assigned a unique identification number. He suggested that EHR in a standard format should be developed and deployed throughout the country by providing an enabling environment. He also mentioned that upcoming technologies such as – Machine to machine technology, Internet of Things (IoT) etc. should be optimally used. On the aspects of electronic health data privacy & security, he mentioned that National Law School of India University from Bengaluru has been assigned the work to come out with a legal framework and draft legislation.
5. **Shri C.K. Mishra, AS & MD** mentioned that the Indian healthcare system is very complex system and technology is the only way to fill the existing gaps between the patients and the medical system. He mentioned about three major challenges in health sector i.e. making health facility & services accessible and affordable as well as maintaining the quality of services. He also said that technology is a good supplement for human resource and knowledge and will play a big role in coming future in the healthcare domain. In order to handle critical factor, i.e., management of healthcare in our country, he further emphasized the need to have strong IT systems in place.
6. **Prof. M.C. Mishra (Director) AIIMS, New Delhi** said that nowadays patients all over the country are generally misusing antibiotics by taking antibiotics without consultation from doctors. He then mentioned about existing system in place at AIIMS which enables to track antibiotic usage by the patients undergoing treatment at AIIMS. With such system in place, they have been able to bring down misuse of antibiotics. He also said that lots of opportunities in collating the EHR records exist in India these days and interoperability of EHR can lead to tremendous time & cost savings for both patients and the health set-ups. He encouraged the use of EHR systems with necessary technology for the benefit of people in long run.
7. **Dr. Rajesh Narwal (WHO, India)** mentioned about the basic supporting pillars of Healthcare and role of ICT in providing access of quality healthcare to everybody. For this ICT can be a key enabler. He emphasized that critical gap of human resources needs to be filled up at that level. There is strong need for integration between the existing as well as newly developed health systems. He also emphasized on the need for interoperability



between healthcare systems across the country for a seamless data & information exchange/transaction between government and private healthcare providers.

8. Dr. Narwal also discussed importance of critical inputs like political & financial support, inter- departmental cooperation and collaboration between states for functioning of regulatory body.
9. **Prof. S.N. Sarbadhikari, Project Director, CHI** made a presentation outlining the Aim, Vision and Goal of NeHA:
  - **Aim:** In order to guide and support India's journey in eHealth and consequent realization of benefits of ICT intervention in Health sector in an orderly way, the Ministry proposes to set up National eHealth Authority (NeHA) as a statutory body for promotional, regulatory and standards related roles.
  - **Vision:** Attainment of high quality health services for citizen through cost-effective and secure use of information and communication technologies in health and health-related fields.
  - **Goal:** To ensure development and promotion of eHealth ecosystem in India for enabling the organization, management and provision of effective people-centric health services to all in an efficient, cost effective and transparent manner.

Prof. Sarbadhikari mentioned that the draft Concept Note on setting up of NeHA was placed in public domain seeking suggestions/comments and more than 500 comments/suggestions were received from various stakeholders, associations, industry players etc., which were very useful for further improving the concept note. He also explained about need for National eHealth Policy for eHealth adoption in the country which includes data management, privacy and security, policy guidelines for health records of patients visiting the health facilities.

10. **Shri Rajendra Pratap Gupta** gave suggestions on standardization of EHR at hospitals, state and micro level. He said nation-wide guidelines should be in place for EHR standards. He also gave an important suggestion on renaming National eHealth Authority to "**National Digital Health Authority**", to keep in line with "Digital India" and also to broaden the scope of the Authority, so that mHealth and Tele-Health also could be included in its purview.
11. **Mr. B S Bedi, Advisor - CDAC** discussed about user acceptability of EHR. He emphasized that for an EHR system to run successfully, it should be made user friendly so as to be acceptable to Doctors / paramedics who would be main operators / users.
12. **Ms. Manisha Mantri, Pune** explained how ICT can help effectively in storing, recording and receiving the sharable and transferable medical records. She briefed the participants on EHR standards, structured terminology, coding systems, Healthcare information exchange,

security, privacy and emphasized much on data security and privacy along with making the whole system on EHR.

13. Presentations of the ongoing eHealth applications were given by four States namely Tamil Nadu, Gujarat, Himachal Pradesh, and, Kerala. The Panel was chaired by Shri Sunil Sharma, JS (eGov), MoHFW and panellists were: i) Shri Sunil Bhushan, STD (NIC), (ii) Shri Srinivasan Ramakrishnan, Advisor, NISG and (iii) Shri Jitendra Arora, Director (eGov), MoHFW.

States highlighted the challenges being faced by them during carrying out eHealth initiatives. They echoed the sentiments that improved healthcare delivery can be improved substantially by providing medical personnel with better access to data, faster data retrieval and higher quality of data.

14. After detailed discussions & deliberations during the consultation, **Shri K. B. Agarwal, AS (eGov.) MoHFW** summarized the discussion points observing that there has been consensus amongst the participants on the proposal for creation of the National e-Health Authority which would lay and regulate standards in the e-Health domain and **catalyze** and promote e-Health initiatives in the country.

15. The consultation ended with vote of thanks to the chair and co-chair and the participants.

**Annexure 1: NeHA Consultation Schedule**

Registration		10:00 – 10:30
Welcome Address	Shri Sunil Sharma, JS (eGov), MoHFW	10:30 – 10:40
Address	Shri C. K. Mishra, AS&MD, MoHFW	10:40 – 10:50
Address	Dr. Aruna Sharma, Secretary, DeitY	10:50 – 11:00
Keynote Address	Shri B. P. Sharma, Secretary (HFW), MoHFW	11:00 – 11:10
Presidential Address	Shri J.P. Nadda, Hon'ble Union Health and Family Welfare Minister	11:10 – 11:25
<b>Tea Break</b>		11:25 – 11:40
Presentation on: - Concept Note of NeHA - Standards in Health Informatics	(i) Prof. S. N. Sarbadhikari, Project Director, CHI	11:40 – 11:50
	(ii) Representative of iNRC (CDAC, PUNE)	11:50 – 12:00
Panel discussion and stakeholder consultation on NeHA : - Role - Structure - Road Map	Panel Chair : Shri K. B. Agarwal, Addl. Secretary(F&D), MoHFW <u>Panel members:</u> (i) Shri Sunil Sharma, JS (eGov), MoHFW (ii) Prof S. N. Sarbadhikari, Project Director, CHI (iii) Representative, WHO India (iv) Representative, DeitY (v) Representative, NISG (vi) Shri B. S. Bedi, Advisor- CDAC	12:00 – 14:00
<b>Lunch</b>		14:00 - 14:30
Experiences of States in implementation of Hospital Information System (HIS) and Interoperability of EHR	Presentation by States (Tamil Nadu, Gujarat, Haryana, Himachal Pradesh, Kerala) Panel Chair: a. Shri Manoj Jhalani, JS(Policy), MoHFW b. Shri Sunil Sharma, JS (eGov), MoHFW	14:30 - 16:00
Vote of Thanks	Shri Ankit Tripathi, Additional Director, CHI	16:00

**Annexure 2 : List of Attendees**

S.No.	NAME	DESIGNATION	ORGANISATION / STATE
1.	Shri B.P. Sharma	Secretary (H&FW)	MoHFW, New Delhi
2.	Dr. Aruna Sharma	Secretary, DeitY	MCIT, New Delhi
3.	Shri C K Mishra	AS & MD (NHM)	MoHFW, New Delhi
4.	Shri K B Agarwal	Addl Secy (F and D)	MoHFW, New Delhi
5.	Prof. M. C. Misra	Director, AIIMS	New Delhi
6.	Dr. B D Athani	Spl. DGHS	MoHFW, New Delhi
7.	Shri Sunil Sharma	JS (e-Gov) MoHFW	MoHFW, New Delhi
8.	Dr. Om Prakash	Principal Secretary	Uttarakhand
9.	Shri Jitendra Arora	Director (e-Gov)	MoHFW, New Delhi
10.	Dr. K K Agarwal	Hony. Secy. General	IMA HQrs., New Delhi
11.	Shri Rajendra Pratap Gupta	Policy Advisor	Mumbai
12.	Dr. Rajesh Narwal	Technical Officer- Health Systems Stewardship & Regulations	WHO (India)
13.	Shri B.S. Bedi	Advisor	C-DAC, Pune
14.	Shri S. Ramakrishnan	Advisor	NISG, New Delhi
15.	Shri Sudhir Saxena	Vice President	NISG, New Delhi
16.	Dr. Jayanta K Das	Director	NIHFW, New Delhi
17.	Shri Rajesh Gera	DDG	NIC, New Delhi
18.	Prof. S.N Sarbadhikari	Project Director, CHI	NIHFW, New Delhi
19.	Dr. S. B. Bhattacharyya	Head- Health Informatics	TCS
20.	Shri Sunil Kumar	Senior Technical Director	NIC, New Delhi
21.	Mrs. Manisha Mantri	iNRC, C- DAC	Pune
22.	Dr. Surya Bali	Nodal officer	Madhya Pradesh
23.	Dr. Karan Vir Singh	Apollo Hospitals	New Delhi
24.	Mr. Arvind Shivaramakrisnan	Apollo Hospitals	Hyderabad
25.	Shri Anjan bose	NatHealth	New Delhi
26.	Shri Ankit Tripathi	Addl Director, CHI	New Delhi
27.	Shri Gaurav Sharma	Deputy Director, CHI	New Delhi
28.	Dr. Sanjay Gupta	Nodal Officer, CHI	NIHFW
29.	Dr. J.K. Shivdasani	Asst. Nodal Officer, CHI	NIHFW
30.	Dr. C. Jayan	Joint director - e-health	Kerala
31.	Smt. Sowjanya	Mission Director, NHM	Karnataka
32.	Shri Sandeep Chopra	Scientist	NIC, New Delhi
33.	Dr. Subodh	Head Surgery	AIIMS, New Delhi
34.	Shri Ajay Rampal	STD, NIC	New Delhi
35.	Shri B.B. Pawar	Deputy Director	Maharashtra

36.	Shri Sameer K. Sinha	Commissioner & Secretary Health Department	Assam
37.	Dr. N.V. Kamatt	Pr. Advisor	IMA (HQ)
38.	Shri B K. Datta	DS.	MoHFW, New Delhi
39.	Shri Abhishek Jain	Manager- HLS	Wipro
40.	Shri Amit Kumar	AD (e-Gov)	MoHFW, New Delhi
41.	Dr. Sunil Srivastava	DG (MH)	Uttar Pradesh
42.	Shri Amarjeet Singh	Director	DGHS
43.	Mr. Anirudh Sen	FICCI	New Delhi
44.	Dr. A. K. Chaudhary	AD. IT	Lucknow
45.	Shri Sunil Gupta	HMIS - IT	Uttar Pradesh
46.	Dr. M.P. Sharma	DGHS Office	Haryana
47.	Dr. Vishwaajeet Singh	DGHS Office	Haryana
48.	Shri Rajesh Sihag	DGHS Office	Haryana
49.	Dr. Neeraj Kharwal	MD, NHM	Uttar Pradesh
50.	Major Sandeep Sharma	Ministry of Defense; IAMI	New Delhi
51.	Lt. Ankur Gupta	AIIMS; IAMI	New Delhi
52.	Shri Ashish Sharma	MoHFW	New Delhi
53.	Dr. Monika Rana	Addl. Secretary GNGT	
54.	Shri Piyush Chaturvedi	Sr. Manager	Mitra India Ltd.
55.	Sm. Vibha Mehra	Head, BD	Wipro
56.	Dr. C. Murli K. Kumar	Advisor Health	Niti Ayog
57.	Dr. Ritesh Mondal		Andaman & Nicobar
58.	Dr. Probin Chandra Arambam	Deputy Director of Health	Manipur
59.	Dr. Ahanthem Victor Singh	Block HMIS officer	Manipur
60.	Shri B.B. Mittal	Dy. Director - Rural Health	Gujarat
61.	Mr. Shahnawaz Khan Rathod	Project officer - IT	Gujarat
62.	Dr. Ganesh	Nodal officer	Karnataka
63.	Shri Suren Kumar	AIIMS – Technical Staff	New Delhi
64.	Shri M. Harish	AIIMS – Technical Staff	New Delhi
65.	Shri Bobby Kumar	AIIMS – Technical Staff	New Delhi
66.	Dr. D.K. Pandu	TLSHSRC, NHM	Odisha
67.	Dr. Sampooran Singh	DHS	Chandigarh, Punjab
68.	Mr. Samuel Lalhmingmawia,	MIS Manager	Mizoram
69.	Sm. Rajbala	Telemedicine AIIMS	New Delhi

70.	Dr. Anita Bhutia	DD/ RCH	Sikkim
71.	Shri K. Srinivas Subramanyam	STC. NHM	Chhattisgarh
72.	Dr. M. Srinivas Rao	State program officer, NHM	Telangana
73.	Shri B. Satyanarayan	IT - department	Telangana
74.	Dr. K. Ravi Krishna Sharma	IIHFW	Telangana
75.	Dr. Amit Sukla	Dy. Director - Rural health	MG education
76.	Mrs. Anand Sharma	Consultant	Uttarakhand
77.	Ms. Charu khattar	DA ( e- gov)	Delhi
78.	Dr. Salim	Director Health	VISK
79.	Dr. Anurupa Roy	Associate Consultant	MoHFW, New Delhi
80.	Mr. Saurabh Kumar	Associate Consultant	NIHFW, New Delhi
81.	Ms. Indu Bala	Associate Consultant	MoHFW, New Delhi
82.	Mr. Biju Raj	Associate Consultant	MoHFW, New Delhi
83.	Dr. J Panday	CHI	NIHFW, New Delhi
84.	Dr. Eswar Das	CHI	NIHFW, New Delhi
85.	Dr. M Alam Khan	CHI	NIHFW, New Delhi
86.	Dr. S Gupta	CHI	NIHFW, New Delhi
87.	Dr. A Rastogi	CHI	NIHFW, New Delhi
88.	Ms. Ginny Bansal	CHI	NIHFW, New Delhi
89.	Ms. Antika Jain	CHI	NIHFW, New Delhi
90.	Ms. Richa Verma	CHI	NIHFW, New Delhi
91.	Ms. Parul	CHI	NIHFW, New Delhi
92.	Mr. Yunus	CHI	NIHFW, New Delhi
93.	Mr. Vijay Krishan	CHI	NIHFW, New Delhi
<b>Many other participants from various States/UTs have also attended this consultation</b>			

## Department of Health &amp; FW

Dated 06/09/2017

I am directed to forward a copy of the Minutes of the Meeting held under the chairmanship of Hon'ble HFM on 19/08/2017. It is requested to submit compliance of directions issued, to Joint Secretary(LA) at the earliest.



(D. Jeevaraj)

PPS to Joint Secretary(LA)

06/09/2017

CMD, HLL  
Director(e-Gov)  
DDG(O)  
DS(ZSV)

vs (eGov)  
Re dring

6/9/17

Office of J.S. (LA)  
File No. 654676  
Date 6/9/17



MINUTES OF THE MEETING HELD UNDER THE CHAIRMANSHIP  
OF HON'BLE HFM ON 19/08/2017

A review meeting was held under the chairmanship of Hon'ble HFM on 19/08/2017 to review the following Programmes:-

1. IT Initiatives
2. Blindness Control Programme
3. Amrit Pharmacies

The following were Present:-

1. Shri C.K. Mishra,  
Secretary, HFW
2. Shri R.K. Vats  
AS&DG
3. Shri Sanjeeva Kumar  
Additional Secretary (Health)
4. Shri Manoj Jhalani  
AS&MD, NHM
5. Shri Lav Agarwal  
Joint Secretary
6. Shri R.P. Khandelwal  
CMD, HLL
7. Shri Jitender Arora  
Director
8. Dr. Promeela Gupta  
DDG(O)
9. Shri Zile Singh Vical,  
DS
10. Shri Ankit Tripathi,  
Dy. Director

I. IT Initiatives

A detailed presentation on e-Health activities was made during the meeting. Various IT initiatives currently in place, their present usage pattern and issues for expansion of the same including inter-operability were highlighted. Further, a number of initiatives which are under



process which include Health information Exchange, Creation of Dash Board, Tele-medicine network were highlighted. Hon'ble HFM and Secretary, Health have accordingly issued the following directions:-

- Though a large number of mobile applications have been launched in the past but their usage by citizen is relatively less. An analysis with respect to utility of these application needs to be taken up. Further, all the mobile Apps should be brought into one Umbrella Health Department Application and action shall be initiated to ensure higher outreach of Umbrella App.
- A policy document shall also be prepared with respect to how and what type of new mobile applications are prepared and launched.
- Division to examine the existing National Medical Library Portal and inclusion of remaining Medical Colleges into membership fold.
- Success stories like e-Vin, Medical Libraries Network and Kilkari shall be highlighted including organizing guided media tree for the same.
- Since only limited users are there on e-Rakt Kosh application of C-DAC, necessary action to close the same may be initiated.
- Draft for National Digital Health Authority Act should be discussed with Ministry of IT and it shall be examined whether we need to have an independent Act for Health Department or it shall be subsumed within the Act being prepared by the Ministry of Electronics and Information Technology.
- Necessary action to expand National Medical College network scheme to cover 50 Medical Colleges shall be initiated besides working out a strategy for extending the same Pan-India.
- Tele-medicine shall be taken up with a view to provide services in peripheral areas in a Mission Mode.

## II. Blindness Control Programme

A detailed Presentation on present status of Blindness, causes of blindness and the proposed concept Note on "Motia bind Mukh Bharat" has been explained. The discussion ensued with respect to working out



the requirement of additional funds so as to launch this programme in a Mission Mode. It was noted that advanced preparation is required to ensure that as and when the Programme is taken up, sufficient capacities be ensured for effective implementation of the Mission mode concept. Accordingly, it was decided that the Division shall take necessary action as follows:-

- Necessary action shall be initiated to create an IT Application for effective monitoring of the same.
- Appropriate mapping of technical manpower at the district level in Government Sector, NGOs and private practitioners be initiated.
- Necessary action to complete the backlog payment for NGOs in consultation with NHM may be initiated with States.
- Further, follow up be done with Ministry of Finance for additional resources for launching it in Mission Mode.

### III AMRIT Pharmacies

A detailed presentation was given on the existing status of Amrit Pharmacies covering 18 States/UTs and the savings accrued to the patients so far. Strategies for rapid expansion in terms of introduction of Franchisee model, inventory management through an Aggregator and online solution for getting orders from website and Mobile application were explained and the following decisions were taken:-

- Necessary action to ensure adequate publicity of Amrit initiatives be taken up
- The proposed Plan of action for increasing the number of Amrit Pharmacies be implemented.
- An efficient and on-line grievance redressal mechanism shall be put in place.
- Proper transparency in terms of purchases is crucial for the success of the programme and hence the same shall be ensured besides creating a robust IT application with effective dash board.

The meeting ended with thanks to the Chair.

\*\*\*\*\*

GistF.No. Z.18015/23/2017-eGov

In order to address the needs identified and delineated for regulation, data privacy and security etc. in Indian e-Health System, it was decided in this Ministry to set up a Nodal Body in the form of an Authority through an Act of Parliament. For drafting the Act, National Law School of India University, Bengaluru was mandated. The draft Act for setting up the Central Authority by name National Digital Health Authority of India has now been finalized (F/M').

2. It was also decided in this Ministry to put the draft Act on public domain for a period of one month seeking suggestions/comments from general public by 31.05.2017. Hon'ble MoS(AP), while taking review meeting with e-Health division on 15.05.2017 had directed that this deadline be met with.

3. This file is put up seeking approval of Hon'ble HFM for putting the Draft Act on Public Domain.

4. Hon'ble MoS(AP) may kindly approved the file to be sent to Hon'ble Minister of Health and Family Welfare.



(Dr. A. Madhavan)  
Sr. Consultant  
25-05-2017



**NATIONAL DIGITAL HEALTH AUTHORITY ACT**  
**Responses from NLSIU, Bengaluru**

**for the comments & clarifications sent by MoHFW on July 14, 2017**

Provisions	Observations/Comments (MoHFW)	Observations (NLSIU)
<b>I. Preamble</b>	<ol style="list-style-type: none"><li>1. Establishment of Adjudicating Authority(ies) and Appellate Tribunal may also be added. [Refer TRAI Act, where similar mention is made]</li><li>2. This Act does not mandate “setting up of Health Information Exchange (HIE)”. It outlines that HIEs will have to be recognised by NDHA.</li></ol>	<ol style="list-style-type: none"><li>1. Incorporated accordingly to the extent possible from the legal perspective.</li><li>2. -----do-----</li></ol>
<b>II. Section 6 ENTITIES TO COLLECT DIGITAL HEALTH CARE DATA AS PER THE PROVISIONS OF THIS ACT</b>	<ol style="list-style-type: none"><li>1. Entities other than Health Service provider or HIE shall be permitted by the National Digital Health Authority of India.</li><li>2. It should be “collecting or storing or transmitting digital health care data”.</li></ol>	<ol style="list-style-type: none"><li>1. It is ideal that the power of ‘notification’ shall lie with the Central Government (under the MoHFW as of now). This is in consonance with other similar statutes.</li></ol>
<b>III. Section 8 (2), (3) &amp; (5) Storing of Digital Health Care Data</b>	<ol style="list-style-type: none"><li>1. De-identification/ anonymization of data generally happens at the point of exit (during transmission of data)</li><li>2. Such technical aspects shall be dealt with under Rules</li></ol>	<ol style="list-style-type: none"><li>1. This part of the statute deals with one of the cardinal principle viz., privacy, confidentiality of the data; and the data collected shall be made available for policy use (i.e., public purpose). Therefore, it is imperative that these principles remain as part of the statute.</li><li>2. Further the power to specify the technical details is being delegated to the NDHAI, which can be formulated as part of Rule Making.</li></ol>



Provisions	Observations/Comments (MoHFW)	Observations (NLSIU)
<b>IV. Section 10 (4) (a) &amp; (b) The Rights of the Owner</b>	<ol style="list-style-type: none"> <li>1. This provision should be only in case of <b>incorrect</b> digital health care data.</li> <li>2. This sub-clause should be re-worded as "The right to require his explicit prior permission for each instance of transmitting or use of his digital health care data in identifiable form, using such means notified by the National Digital Health Authority"</li> </ol>	<ol style="list-style-type: none"> <li>1. The said changes have been incorporated accordingly.</li> <li>2. The comment is correct. But the attempt of this provision is to articulate the right of an owner. Therefore, no change is required.</li> </ol>
<b>V. Section 11(1)(f) The duties of the Health Service Provider or Health Information Exchange</b>	<ol style="list-style-type: none"> <li>1. A copy of data should be provided back to owner. Accordingly the wording should be modified.</li> </ol>	<ol style="list-style-type: none"> <li>1. The said changes have been incorporated accordingly.</li> </ol>
<b>VI. Section 13 (2) &amp; (4) Transmission of Data</b>	<ol style="list-style-type: none"> <li>1. NDHAI may prescribe required technical standards for data transmission, including the aspect of transmitted data to be de-identified</li> <li>2. It should be part of Rules to be defined by NDHAI</li> </ol>	<ol style="list-style-type: none"> <li>1. The suggestion and the earlier provision are merely using different language. However, there is delegation of power to NDHAI and law (Administrative Law) requires the delegation of power shall be with proper guidance. Therefore, the original version is retained.</li> <li>2. The rule will detail out the technical details. However, the requirement is that the power to detail out needs to be delegated. Therefore, the original version is retained.</li> </ol>
<b>VII. Section 17 Composition of NDHAI</b>	<ol style="list-style-type: none"> <li>1. Appointment of Members shall be by Central Government ; Ex-officio members (3-4): JS (MoHFW), JS (IT), JS (Law); Secretariat shall have a Secretary (Director level officer)</li> </ol>	<ol style="list-style-type: none"> <li>1. As the Expert Committee opines to have three/four members in their ex-officio capacity, there is no need to have any further qualifications for them under sub-section (3). However, for the appointment of the Chairman and four full time members the qualifications shall apply. The option of the government would be</li> </ol>



Provisions	Observations/Comments (MoHFW)	Observations (NLSIU)
	2. Section 17 (2) – NDHAI may co-opt Experts on need basis for fixed term.	<p>broad if more areas are there. Moreover, the chair is expected to have true statesmanship in handling things.</p> <p>2. The said changes have been incorporated accordingly.</p>
<b>VIII. Term of office of Chairman &amp; other members</b>	<p>1. may be sixty five years</p> <p>2. The co-opted member shall hold office at the pleasure of the Authority, not exceeding two years from the date of appointment.[not required]</p>	<p>1. The said changes have been incorporated accordingly.</p> <p>2. The said changes have been incorporated accordingly.</p>
<b>IX. Section 24 Powers and Functions of NDHAI</b>	1. To assign power to NDHAI also to take punitive actions in case of default/breach etc.	1. The punitive actions are the privilege of courts and can't be abdicated by semi-regulatory authority like NDHAI. The example of TRAI does not hold good.
<b>X. Section 39(1) (b), (2) (c) THE BREACH OF DIGITAL HEALTH CARE DATA</b>	<p>1. May like to redraft as: "If digital health care data is not stored or transmitted by any HIE or HSP as per the norms under this Act or the standards laid down by NDHAI."</p> <p>2. What is meant by "serious digital health care data"? It shall be defined.</p> <p>3. Entities having data where breach has occurred should notify NDHAI &amp; also Individual, as case may be.</p>	<p>1. The said changes have been incorporated accordingly.</p> <p>2. Section 39 (2) is self-explanatory. Therefore, the original version is retained.</p> <p>3. The said changes have been incorporated accordingly by incorporating a separate provision i.e., Section 39 (3).</p>
<b>XI. Section 41 Penalty for failure to furnish information, return etc.,</b>	1. Provision of penalty for failure to observe Rules or Directions by NDHAI shall be added.	1. Section 41 is self-explanatory and also covers the requirements of NDHAI to be observed by any person or Health Information Exchange. Therefore, the original version is retained.

**Note:** Few of the suggestions do not carry sufficient merit (from jurisprudential point of view) for incorporation in the draft.

**NATIONAL LAW SCHOOL OF INDIA UNIVERSITY**

NAGARBHAVI, BENGALURU - 560 242

Telephone : +91 80 2316 0537

Email : registrar@nls.ac.in, ovnandimath@nls.ac.in

**O.V. Nandimath** *Ph.D**Registrar & Professor of Law*

No. NLSIU-22022/3/2016-ADMN

September 15, 2017

Dear Sir,

This has reference to your letter No. Q-11013/6/2015-eGov dated 11<sup>th</sup> February 2016, regarding drafting of 'National Digital Health Authority of India Act;' and the last Expert Committee meeting held on 14<sup>th</sup> July, 2017 at New Delhi. In this regard, may I submit as follows,

1. The final revised draft incorporating all the suggestions made till now is appended herewith;
2. Few of the suggestions does not carry sufficient merit (from jurisprudential point of view) for incorporation in the draft. A matrix indicating the reason for the same is also being appended for your ready reference;
3. With this milestone, NLSIU's obligation as per the MoU dated 15<sup>th</sup> February 2016 is complied with;

Necessary invoice and statement of expenditure for final release of payment and other incidental expenses are enclosed. For other incidental charges we have already sent statement of expenditure which is also due for payment. This is for your kind information and further needful.

Thanking you,

Yours sincerely,

Nandimath O.V.

To  
Shri. Jitendra Arora  
Director  
Ministry of Health and Family Welfare  
e-Governance Section  
Government of India  
Nirman Bhavan, New Delhi-110 011

**INDEX**

<b>SL. NO.</b>	<b>PARTICULARS</b>	<b>PAGE NO.</b>
1	CHAPTER I – PRELIMINARY	2
2	CHAPTER II - DATA OWNERSHIP, SECURITY AND STANDARDIZATION	8
3	CHAPTER III - NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA	21
4	CHAPTER IV- HEALTH INFORMATION EXCHANGE	30
5	CHAPTER V- DIGITAL HEALTH CARE DATA BREACH AND CONSEQUENCES	43
6	CHAPTER VI- ADJUDICATING AUTHORITY AND APPELLATE AUTHORITY	49
7	CHAPTER VII- MISCELLANEOUS PROVISIONS	66



**NATIONAL DIGITAL HEALTH AUTHORITY OF  
INDIA ACT, (INSERT YEAR)**

---

*An Act to provide for establishment of National Digital Health Authority of India, and Adjudicating Authority(ies) and Appellate Tribunal; and to provide for recognition to Health Information Exchanges and further to provide for effective digital health care data privacy, confidentiality, security and standardization; and such other matters related and incidental thereto.*

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

**CHAPTER I  
PRELIMINARY**

---

**1. SHORT TITLE, EXTENT**

- (1) This Act may be called as National Digital Health Authority of India Act, (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

**2. COMMENCEMENT AND APPLICATION**

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.

- (2) Save as otherwise expressly provided by the Central Government by Notification, this Act shall apply to all digital medical records, digital health records or digital personal/protected health data as the case may be.

### **3. ACT TO SUPERSEDE ANY OTHER LAW**

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health care data' hereunder.

### **4. DEFINITIONS**

- (1) In this Act, unless the context otherwise requires,
  - (a) **'Anonymization'** means the process of permanently eliminating the identity of the owner and his/her digital health data, which may include removal of names or address or numbers or marks or telephone number or such government issued identification number or card etc.
  - (b) **'Breach'** means and includes the breach of digital health care data as per section 39 of this Act.

- (c) **‘Consent’** means informed consent by the owner for collection or storage or dissemination of digital health care data already collected or to be collected and shall include subject to the circumstances envisaged under this Act, proxy consent on behalf of the owner.
- (d) **‘De-identification’** means and includes the process of removing or obscuring any personally identifiable information from individual health-data in a manner that eliminates the risk of unintended disclosure of the identity of individuals and health information about them.
- (e) **‘Digital Health Care Data’** is any data about the individual collected and/or recorded digitally in the course of provisioning of health services to the individual or otherwise, by the Health Service Provider or Health Information Exchange, and the said expression shall mean and specifically include the following:
  - (i) All data pertaining to the health status of the owner;

- (ii) All information collected about the individual during the process of registration to provide health services;
  - (iii) Information about payments or eligibility for healthcare with respect to the individual;
  - (iv) A number, symbol or such other particular assigned to an individual to uniquely identify the individual for health purposes;
  - (v) Information derived from the testing or examination of a body part or bodily substance, including biological samples;
  - (vi) Identification of person as provider of health care to the individual;
  - (vii) Any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.
- (f) **‘Entity’** means a person, or a partnership, or any other incorporated or

unincorporated association or body; or a trust or part of an entity.

- (g) **‘Guardian’** means a parent or spouse or brother or sister or any relative or in some circumstances an attendant or person appointed by Court or such other person to be specified.
- (h) **‘Health Informatics’** – the expression shall generically mean and include interdisciplinary study of the design, development, adoption, and application of information technology based innovations in healthcare services delivery, management, and planning.
- (i) **‘Health Information Exchange’** means Health Information Exchange as recognized under this Act.
- (j) **‘Health Service Provider’** is an entity registrable under sub-section (c) of Section 2 of Clinical Establishment (Registration & Regulation) Act, 2010, as a ‘Clinical Establishment’; or any other equivalent law for the time being in force and such other entity or class of entities which Central Government shall declare by Notification.

- (k) **‘Owner’** is an individual to whom the digital health care data belongs to, as per Section 5 of the Act.
- (l) **‘Prescribed’** shall mean rules prescribed by the Central Government.
- (m) **‘Privacy’** is a right of an individual as recognized by Indian Courts and specifically mean to suggest (to this statute) the right of an individual to control or influence what digital health care data related to him may be collected or stored or transmitted by whom, or how and when and to whom that digital health care data may be disclosed.
- (n) **‘Security’** refers directly to protection, and specifically to the means used to protect the privacy of health information and support professionals in holding that information in confidence.
- (o) **‘Specified’** shall mean as specified by National Digital Health Authority of India.
- (p) **‘Transmission of Digital Health Care Data’** shall mean transmission of Digital health care data, for the purposes of this Act, and means to communicate the digital health care data or to release it to another.

## **CHAPTER II**

### **DATA OWNERSHIP, SECURITY AND STANDARDIZATION**

---

#### **5. OWNERSHIP OF DIGITAL HEALTH CARE DATA**

- (1) The Digital health care data generated or collected or transmitted shall be owned by the individual to whom the digital health care data belongs to;
- (2) Health Service Provider or Health Information Exchange shall hold such digital health care data referred to in subsection (1) above in trust for the owner;
- (3) Notwithstanding anything stated above in this section, the medium of storage and transmission of digital health care data shall be owned by the Health Service Provider or Health Information Exchange as the case may be.

#### **6. ENTITIES TO COLLECT DIGITAL HEALTH CARE DATA AS PER THE PROVISIONS OF THIS ACT**

- (1) Health Service Provider or Health Information Exchange shall collect or store or transmit either within India or abroad any digital health care data, strictly as per the provisions of this Act.
- (2) Further, entities other than the Health Service Provider or Health Information Exchange collecting or storing or transmitting digital

health care data either within India or abroad, shall be notified by the Central Government for the purposes of this Act.

## **7. COLLECTION OF DIGITAL HEALTH CARE DATA**

- (1) Health Service Provider or Health Information Exchange, as the case may be, shall by express consent from the owner lawfully collect the required digital health care data as per the prescribed norms by the National Digital Health Authority of India, subsequent to, adequately informing the owner;
  - (a) The purpose of collection of such health data;
  - (b) The digital health care data to be collected;
  - (c) The entity or group or individual to whom the digital health care data shall be transmitted or disclosed;
  - (d) The entity or group or individual who shall have access to such collected digital health care data.
  - (e) The rights of the owner over the digital health care data as described in this Act.
- (2) Without prejudice to sub-section (1) above, the digital health care data can be collected by Health Service Provider or Health Information Exchange as the case may be, of an individual



who is incapacitated or incompetent to provide consent, by obtaining proxy consent from spouse or parent or legal guardian or attendant or such other person to be prescribed.

**Explanation 1:** For the removal of any ambiguity it is stated that, in case of proxy consent the person providing proxy at the time of contingency, shall have legal capacity to consent for the process of obtaining digital health care data of an individual.

**Explanation 2:** In case of temporary health scenarios the consent of the digital health care data owner may be taken once the person is back in to sensibility of legally consenting and exercising the legal rights.

- (3) National Digital Health Authority of India may prescribe suitable norms in this regard by Notification.

## **8. STORING OF DIGITAL HEALTH CARE DATA**

- (1) Subject to the requirements and restrictions under this Act, digital health care data shall be stored, with Health Service Provider or Health Information Exchange, as the case may be, in accordance with the prescribed standards by the National Digital Health Authority of India in consultation with the Central Government.

- (2) Further, the digital health care data collected and stored as per sub-section (1) above, with Health Service Provider or Health Information Exchange, shall be de-identified or anonymized, as the case may be, to ensure the right to privacy & confidentiality of the owner, by adopting such means or methods as may be prescribed.
- (3) Notwithstanding anything stated in this Act, or any other statute in force, all de-identified and anonymized digital health care data stored as per this Act, shall be deemed to be held by the concerned Health Service Provider or Health Information Exchange, as the case may be on behalf of National Digital Health Authority of India; and such digital health care data be used for such analysis or prediction of spread of diseases or prevalence of diseases or policy formation or such other purposes, without compromising the privacy or confidentiality of the owner.

Provided further that, the digital health care data shall vest with National Digital Health Authority of India, immediately after the death of the owner of the digital health care data.

- (4) The digital health care data vested with National Digital Health Authority as per sub-section (3) above, shall be stored or transmitted or used in such a manner as may be prescribed by the National Digital Health Authority of India in consultation with the Central Government.
- (5) The digital health care data vested with National Digital Health Authority of India as per sub-section (3) above shall not be transmitted or be used, if such transmission or use places the successor or decedents as the case may be, of deceased to plausible stigma.

Provided further that, National Digital Health Authority of India may specify norms by Notification in this regard.

## **9. ACCESS TO DIGITAL HEALTH CARE DATA WITHIN HEALTH SERVICE PROVIDER**

- (1) The digital health care data collected or stored or received by Health Service Provider or Health Information Exchange as the case may be shall be accessed by only such professionals or otherwise, on need to know basis.

**Explanation:** for eliminating any ambiguity it is stated that, without prejudice to sub-section (1) above, within Health Service Provider or Health

Information Exchange as the case may be collecting digital health care data for the purposes of this Act, the concerned doctor or specialist or professional nursing staff or such other professional class of people to be prescribed, examining or performing such other related activities shall only have access to the digital health care data.

- (2) Notwithstanding anything stated in this Act, the immediate family member of an owner may have access to digital health care data during health emergencies;
- (3) Notwithstanding anything stated in this Act, in case of investigation into cognizable offences, digital health care data related information, may be accessed for the purposes of investigation by the investigating authority with the order of the Competent Court;
- (4) Health Service Provider or Health Information Exchange as the case may be, shall maintain the register in digital form to record the purposes and usage of digital health care data accessed within such Health Service Provider or Health Information Exchange, in the prescribed form by the National Digital Health Authority of India.

## 10. THE RIGHTS OF THE OWNER

- (1) The owner shall have the right to deny collection of digital health care data at any time of such collection, subject to Public order and Public Health Emergency scenarios as notified by the Central Government.
- (2) The owner of the digital health care data shall have the right to know the data collected is relevant to the health service sought; and no excess data is collected.
- (3) The owner of the digital health care data shall have the right to know the entities who shall have access to and to whom the digital health care data shall be transmitted or disclosed.
- (4) The owner of the digital health care data shall have, subject to sub-section (1) to (3) above:
  - (a) The right to withdraw or seek for rectifying incorrect digital health care data; or
  - (b) The right to convert the digital health care data into de-identified data; or
  - (c) The right to seek for erasing or rectification of the incorrect digital health care data stored, from the respective Health Service Provider or Health Information Exchange in the prescribed form notified by the National Digital Health Authority of India.

## **11. THE DUTIES OF THE HEALTH SERVICE PROVIDER OR HEALTH INFORMATION EXCHANGE**

- (1) Except where this Act provides otherwise, the Health Service Provider or Health Information Exchange shall be bound to follow the mandate and standards prescribed under this Act in
  - (a) Collecting the digital health care data from an individual as prescribed under this Act;
  - (b) Storing the digital health care data securely by adopting prescribed standard norms;
  - (c) Allowing access to such collected data to only on 'need to know basis';
  - (d) Maintaining digital records of collected digital health care data in a prescribed manner, to access records for future retrieval;
  - (e) Not to transmit the data any further in contravention of this Act and regulate thereunder;
  - (f) Providing a copy of the digital health care data back to the owner on demand made in the prescribed format;
  - (g) Providing proper notice immediately or within three working days to the owner

whenever any digital health care data breach takes place;

## **12. THE PROCEDURE FOR RETRIEVAL OR ANONYMIZATION OF DIGITAL HEALTH CARE DATA BY THE OWNER**

- (1) The owner of the digital health care data shall have an inalienable right to retrieve his digital health care data by making an application in a prescribed form to the Health Service Provider or Health Information Exchange as the case may be;
- (2) On such application under sub-section (1) by the owner for retrieval, the Health Service Provider or Health Information Exchange as the case maybe, shall provide such digital health care data requisitioned immediately or within the same date of such requisition.

**Provided** that, in case of emergency the requisitioned digital health care data may be provided immediately without any delay.

- (3) The owner of the digital health care data shall have the right to seek for erasing or rectifying the incorrect digital health care data stored in any Health Service Provider or Health Information Exchange as the case may be.

Provided further that, the Health Service Provider or Health Information Exchange shall erase such digital health care data immediately or within three working days counted from the date of receipt of such application and the same shall be intimated to the owner.

### 13. TRANSMISSION OF DATA

- (1) The digital health care data collected by Health Service Provider or Health Information Exchange as mentioned under this Act be transmitted with encryption to the designated Health Information Exchange or Health Information Exchanges.
- (2) Without prejudice to foregoing sub-section the digital health care data be transmitted securely and instantaneously after retaining a copy of the same for reasonable use by the Health Service Provider or Health Information Exchange as the case may be.

**Provided** that such transmitted data is de-identified at the Health Information Exchange. Further, for such secure and instantaneous transmission of digital health care data National Digital Health Authority of India may prescribe such technical standards, keeping



the privacy and confidentiality of the owner in mind, by notification.

- (3) The Health Service Provider shall have such digital health care data pertaining to an individual, transmitted to him, upon express consent from the owner.

**Provided** the National Digital Health Authority of India may prescribe standards and such other norms for this transmission of digital health care data between Health Information Exchange and Health Service Provider.

- (4) The Health Information Exchange shall maintain a Register in a prescribed format containing all details of the transmissions of the digital health care data between Health Information Exchange/s and Health Service Provider or between Health Information Exchanges.

#### **14. THE PROCEDURE OF TRANSMISSION OF DATA**

- (1) Without prejudice to any other provisions in this Act, the National Digital Health Authority of India shall prescribe the standards or norms for transmission of digital health care data.

- (2) The National Digital Health Authority of India shall prescribe standards or norms under sub-section (1) above for
- (a) Transmission of digital health care data between Health Service Provider to Health Information Exchange or Health Information Exchanges; or
  - (b) Transmission of digital health care data between Health Information Exchanges per se; or
  - (c) Transmission of digital health care data between Health Information Exchange or Health Information Exchanges and Health Service Provider.

## **15. STANDARDIZATION OF DIGITAL HEALTH CARE DATA**

- (1) Notwithstanding anything stated in this law or in any other law for the time being in force, the National Digital Health Authority of India shall prescribe standards in collecting, storing, transmitting the digital health care data and any other standards required for the said purposes under this Act;
- (2) Provided further that, the Health Service Provider or Health Information Exchange shall implement standards as prescribed by the National Digital Health Authority of India to:

- (a) Ensure the confidentiality, integrity, and availability of all the digital health care data created, transmitted, received, or maintained;
- (b) Protect against reasonably anticipated threats or hazards to the security of the health care data;
- (c) Protect against uses or disclosures of the digital health care data that are not required or permitted under the prescribed standards;
- (d) Ensure their personnel to comply with their security policies and procedures.

**CHAPTER III**  
**NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

---

**16. NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

- (1) The Central Government shall establish the National Digital Health Authority of India by Notification, which may be referred to as National Digital Health Authority of India in its abbreviated form.
- (2) The National Digital Health Authority of India shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government specifies a separate date in the same Notification.

**17. COMPOSITION OF NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

- (1) National Digital Health Authority of India shall consist of the following members, to be appointed by Central Government by Notification, namely:
  - (a) A full time Chairman;
  - (b) Four full-time members to be appointed by the Central Government,
  - (c) Three ex-officio members, to be appointed by the Central Government, shall be Joint Secretary (MoHFW), Joint Secretary (IT), Joint Secretary (Law).

- (d) A Secretary, of Director level officer, to be appointed at the Secretariat.
- (2) Provided that, National Digital Health Authority of India may co-opt experts on need basis for fixed term not exceeding ten at any given point of time, who shall contribute specialized domain knowledge or need or expertise as the case may be.
- (3) Without prejudice to anything stated above, the Chairman and four full time members shall have the following qualifications:
  - (a) Be not less than forty years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Ten years in any of the following areas,
    - (i)Information Technology (IT); or
    - (ii)Health Informatics; or
    - (iii)Medicine; or
    - (iv)Judiciary; or
    - (v) Clinical care; or
    - (vi)Public Health; or
    - (vii)Health Service Delivery; or
    - (viii)Health systems related research; or
    - (ix)Related Academics; or
    - (x)Law; or
    - (xi)Public policy.

**Provided** that, to be appointed as Chairman, the person shall additionally have demonstrable qualities of leadership, institution building and cause of commitment.

- (c) Provided further that, a person shall be disqualified for appointment as per sub-section (1) above, if he –
- (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (ii) Is an undercharged insolvent; or
  - (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
  - (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
  - (v) Has such other disqualification as may be prescribed by the Central Government.

## **18. TERM OF OFFICE OF CHAIRMAN & OTHER MEMBERS**

- (1) The Chairman and other members shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty five years, whichever is earlier.
- (2) The Chairman and other Members, appointed as per sub-section (3) of section 17, are eligible for reappointment for another term or such other terms as the case may be; provided such reappointed Chairman or Member does not exceed sixty five years of age.

## **19. SALARY, ALLOWANCE, BENEFITS AND SERVICE CONDITIONS ETC.,**

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairman and full-time members shall be such as may be prescribed.
- (2) Notwithstanding anything stated in sub-section (1) above, the salary, allowances and other conditions of service of the Chairman or of a member shall not be varied to his disadvantage after his appointment.

- (3) Co-opted additional members, appointed as per sub-section (2) of section 17 shall receive such allowances as may be prescribed.

## **20. RESIGNATION, REMOVAL OF CHAIRMAN OR MEMBER**

- (1) The Chairman or full time member appointed under sub-section (1) of section 17
  - (a) May relinquish his office by submitting the resignation in writing to the Central Government; or
  - (b) May be removed from his office in accordance with the provisions of section 22.
- (2) The Co-opted member appointed as per sub-section (2) of section 17 may relinquish his office by submitting the resignation in writing to the Chairman;
- (3) The Chairman or any full-time member ceasing to hold office as per sub-section (1) above shall not accept any commercial employment, for a period of two years from the date of relinquishment, unless the Central Government exempts him from this disability.



## **21. RECONSTITUTION OF THE AUTHORITY**

Any vacancy caused to the office of the Chairman or any other member shall be filled up by the Central Government immediately or within a period of three months from the date on which such vacancy occurs.

## **22. REMOVAL IN CERTAIN CIRCUMSTANCES**

- (1) The Central Government may remove from office the Chairman or any full-time member, who –
  - (a) Has been adjudged as an insolvent; or
  - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (c) Has become physically or mentally incapable of acting; or
  - (d) Has acquired such financial or other interest as is likely to affect prejudicially his functions as the Chairman or member; or
  - (e) Has so abused his position as to render his continuance in office prejudicial to the public interest.
- (2) No such member or Chairman shall be removed from his office under clause (d) or clause (e) of sub-section (1) above, unless he has been given a reasonable opportunity of being heard in the matter.

### **23.OFFICERS AND OTHER EMPLOYEES OF THE AUTHORITY**

- (1) The National Digital Health Authority of India in consultation with Central Government may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (2) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the Authority appointed under sub-section (1) shall be such as may be prescribed.

### **24.POWERS AND FUNCTIONS OF NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA**

- (1) The National Digital Health Authority of India to ensure confidentiality and privacy of digital health care data shall have the following powers and functions
  - (a) Grant of recognition to such Health Information Exchanges, which fulfill the criteria prescribed.
  - (b) Formulate standards for the collection or storage or transmission of the digital health care data;
  - (c) Lay down the operational guidelines or protocols for the collection or storage or transmission of the digital health care

- data or such other said purposes under this Act;
- (d) Establish the procedure for the collection or storage or transmission of the digital health care data or such other said purposes under this Act;
  - (e) Notify and mandate the Health Service Providers or Health Information Exchanges as the case may be, in case of failure to comply with the provisions of this Act;
  - (f) Conduct investigations to ensure the compliance with any of the provisions of this Act;
  - (g) To act as focal agency in processing the transmission of digital health care data to abroad;
  - (h) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
  - (i) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.

## **25. OVERSIGHT, INSPECTION, ISSUANCE OF DIRECTIONS ETC.**

- (1) To carry out all or any of the powers and functions enumerated in Section 24, the National Digital Health Authority of India shall have the right to inspect all such records; or access the premises, including virtual premises of the Health Information Exchange and Health Service Provider at any time.

**Provided** that National Digital Health Authority of India while accessing such records or accessing either the physical or virtual premises of Health Information Exchanges and Health Service Providers, shall bear in mind that no or least possible hindrance is caused to the normal working of the Health Information Exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Digital Health Authority of India to generally discharge its functions under this Act, shall direct a Health Information Exchange and Health Service Provider, or class of Health Information Exchanges, or all Health Information Exchanges as the case may be, to submit such records or file such returns within such time

and in such manner as specified from time to time.

- (3) All directions under this section issued by the National Digital Health Authority of India are binding upon the Health Information Exchange or Health Information Exchanges and Health Service Providers as the case may be.

## **Chapter IV**

### **HEALTH INFORMATION EXCHANGE**

---

#### **26. RECOGNITION OF HEALTH INFORMATION EXCHANGE**

- (1) No entity shall operate as Health Information Exchange in India, unless duly recognized by the National Digital Authority of India.
- (2) Any Health Information Exchange, which is desirous of operating as such for the purposes of this Act, may make an application in the prescribed manner to the National Digital Health Authority of India.
- (3) Every application under sub-section (2) shall contain such particulars as may be prescribed.

#### **27. GRANT OF RECOGNITION**

- (1) If the National Digital Health Authority of India is satisfied, after making such an inquiry as may be necessary in this behalf and after obtaining such further information, if any, as it may require; but satisfying itself that if granted

recognition privacy and confidentiality of the digital health care data will sufficiently be protected, may grant recognition to such Health Information Exchange.

- (2) Without prejudice to sub-section (1) above, National Digital Health Authority of India may grant recognition subject to such condition or conditions as it may desire.
- (3) Every grant of recognition to the Health Information Exchange under this Section shall be published in the Gazette of India; and such recognition shall have effect as from the date of its publication in the Gazette of India.
- (4) No application for grant of recognition shall be refused except after giving an opportunity to the applicant concerned to be heard in the matter; and the reasons for such refusal shall be communicated in writing.
- (5) Any person aggrieved by either grant of recognition or refusal of recognition as per sub-section (4) above, may prefer an appeal to the Central Government, within thirty days.

**Provided** the Central Government may relax the limitation period of thirty days, if there is justifiable cause for the aggrieved person for not filing his grievance within thirty days, by an

order in writing by assigning reason for such relaxation.

## **28. WITHDRAWAL OF RECOGNITION**

If the National Digital Health Authority of India is of the opinion that the recognition granted to a Health Information Exchange under the provisions of this Act shall, in the interest of digital health care data collected or stored or transmitted or in the public interest, be withdrawn – may serve a written notice of 30 days that, the National Digital Health Authority of India is considering the withdrawal of the recognition for the reasons stated in the notice, and after giving an opportunity to the concerned Health Information Exchange to be heard in the matter, may withdraw by Notification in the Official Gazette, the recognition granted to the Health Information Exchange.

## **29. THE MANAGEMENT OF HEALTH INFORMATION EXCHANGES**

- (1) All Health Information Exchanges, recognized under Section 26, shall conduct and carry out its affairs strictly as per the norms and standards prescribed by the National Digital Health Authority of India from time to time.
- (2) Without prejudice to any other stipulations of this Act, the Health Information Exchange recognized under section 26 shall only employ such skilled personnel for management of its

affairs as may be specified by the National Digital Health Authority of India.

### **30. THE CHIEF HEALTH INFORMATION EXECUTIVE (CHIE)**

- (1) The Health Information Exchange recognized under this Act, shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the National Digital Health Authority of India.
- (2) The Chief Health Information Executive as appointed under sub-section (1) above, shall be the Chief Executive Officer and also the data controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs.

### **31. FUNCTIONS OF THE CHIEF HEALTH INFORMATION EXECUTIVE**

Being the Chief Executive Officer of the Health Information Exchange, he shall –

- (1) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
- (2) Access and transmit and process the digital health care data transmitted by the Health Service Providers to further transmit the digital health care data, whenever required, in



accordance with norms prescribed by the National Digital Health Authority of India.

- (3) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
- (4) Notify the data breach to the owner and such other concerned.
- (5) Store the digital health care data in de-identified or anonymized mode as the case may in all situations.

### **32. POWERS AND RESPONSIBILITIES OF THE CHIEF HEALTH INFORMATION EXECUTIVE**

- (1) The Chief Health Information Executive shall be deemed to be endowed with all such powers to carry out efficiently and effectively all the functions indicated in Section 31 of the Act.
- (2) The Chief Health Information Executive shall be directly held responsible to ensure that all the indicated functions in Section 31 are carried out effectively and efficiently.

### **33. DE-IDENTIFIED DIGITAL HEALTH CARE DATA KEY AND ANONYMIZED DIGITAL HEALTH CARE DATA**

- (1) The Chief Health Information Executive of the Health Information Exchange shall hold the key to link the de-identified data to the individual to whom the digital health care data belongs.

- (2) The key referred to in sub-section (1) shall be held securely by the Chief Health Information Executive, and establish the link while transmitting the digital health care data securely to other Health Information Exchange or Health Service Provider as the case may be.
- (3) The Chief Health Information Executive shall be the officer responsible to permanently destroy the link or key as the case may be, which shall establish the digital health care data's link with its owner, immediately after the receipt of information of owner's death by him.

**Provided** that the Central or State Government shall have access to both de-identified and anonymized digital health care data (without the identity key) from Health Information Exchange or Health Information Exchanges for the formulation of policy purposes.

#### **34. PERIODICAL REPORTS, DIRECT INQUIRIES ETC.**

- (1) Every recognized Health Information Exchange shall furnish to National Digital Health Authority of India such periodical returns relating to its affairs as may be prescribed.
- (2) Every recognized Health Information Exchange shall maintain and preserve for such periods as may be prescribed, the digital health care data

and such other books of accounts; and other documents as the National Digital Health Authority of India may prescribe, and such digital health care data or books of accounts or such other documents shall be subject to inspection at all reasonable times by the National Digital Health Authority of India.

(3) Without prejudice to anything stated in subsection (1) and (2) above, the National Digital Health Authority of India, if it is satisfied that it is in the interest of better implementation of this Act or in the public interest so to do, may by order in writing –

- (a) Call upon the Health Information Exchange or Health Information Exchanges thereof to furnish in writing such information or explanation relating to the affairs of the Health Information Exchange concerned as the National Digital Health Authority of India may require; or
- (b) Appoint one or more of its Member or Members or person or persons to make an inquiry in the prescribed manner in relation to the affairs of the Health Information Exchange or Health Information Exchanges; and submit a

report of the result of such inquiry to National Digital Health Authority of India, within such time as may be specified in the order.

- (c) To have an inquiry conducted independently by the concerned Health Information Exchange or Health Information Exchanges, and submit the report to National Digital Health Authority of India, for further action or otherwise.
- (4) Where an inquiry in relation to the affairs of a recognized Health Information Exchange regarding its affairs has been undertaken under sub-section (3) above –
  - (a) Every director, manager, secretary or other officer of such Health Information Exchange;
  - (b) Every member of such Health Information Exchange;
  - (c) If the member of the Health Information Exchange is a firm; every partner, manager, secretary or other officer of the firm; and
  - (d) Every other person or body of persons who has had dealings in the course of business with any of the persons mentioned in

clauses (a), (b) and (c), whether directly or indirectly –

Shall be bound to produce before the authority making the inquiry all such books of account, and other documents in his custody or power relating to, or having a bearing on the subject-matter of such inquiry and also to furnish the authorities within such time as may be specified with any such statement or information relating thereto as may be required of him.

### **35.ANNUAL REPORTS TO BE FURNISHED TO NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA BY HEALTH INFORMATION EXCHANGE**

Every recognized Health Information Exchange shall furnish to the National Digital Health Authority of India a copy of the annual report, and such annual report shall contain such particulars as may be specified.

### **36.POWER TO ISSUE DIRECTIONS**

- (1) Either generally or after an inquiry as indicated in this Act, the National Digital Health Authority of India, is satisfied that it is necessary in the interest of better implementation of this Act, or accomplish the objectives of this Act or in the public interest, may issue such directions to the Health

Information Exchange or class of Health Information Exchanges as the case may be.

(2) Without prejudice to anything stated in subsection (1) above, the power to issue directions by National Digital Health Authority of India, shall generally encompass the following –

- (a) In the interest of owners of digital health care data;
- (b) To prevent the affairs of Health Information Exchange or Health Information Exchanges, being conducted in a manner detrimental to the overall public interest or the objectives of this Act;
- (c) To secure the proper management of storage and dissemination of digital health care data within the territory of India or abroad;

### **37. POWER TO SUSPEND THE BUSINESS OF RECOGNIZED HEALTH INFORMATION EXCHANGE**

(1) If in the opinion of the National Digital Health Authority of India, an emergency has arisen and for the purpose of meeting the emergency the National Digital Health Authority of India considers it expedient so to do, it may, by notification in the Official Gazette, for the reasons to be set out therein, direct a

recognized Health Information Exchange to suspend such of its business for such period not exceeding thirty days and subject to such conditions as may be specified in the Notification; and if in the opinion of the National Digital Health Authority of India, in the public interest that the period of suspension should be extended, may by Notification, extend the said period from time to time.

- (2) Without prejudice to sub-section (1) above, where the period of suspension is to be extended beyond the first period of thirty days, no Notification extending the period of suspension shall be issued unless the Central Government is consulted.

### **38. POWER OF THE NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA TO SUPERSEDE THE GOVERNING BODY OF A RECOGNIZED HEALTH INFORMATION EXCHANGE**

- (1) Without prejudice to any other powers vested in the National Digital Health Authority of India under this Act, where the National Digital Health Authority of India is of the opinion that the governing body, by whatever name called, of any Health Information Exchange, should be superseded, then notwithstanding anything

contained in any other law for the time being in force, the National Digital Health Authority of India, may supersede the governing body of the Health Information Exchange.

- (2) No superseding as envisaged under sub-section (1) above can take place, unless a written notice that, the National Digital Health Authority of India is considering the supersession of the governing body for the reasons specified in the notice and after giving an opportunity to the governing body to be heard in the matter, and by notification in the Official Gazette, declare the governing body of such Health Information Exchange to be superseded, and appoint any person or persons to exercise and perform all the powers and duties of the governing body, and where more persons than one are appointed, may appoint one of such persons to be the Chairman.
- (3) Immediately on the publication of a notification in the Official Gazette under sub-section (2) above, the following consequences shall ensue –
  - (a) The members of the governing body which has been superseded shall as from the date of notification of supersession, cease to hold office as such members;



- (b) The person or persons appointed under sub-section (1) may exercise and perform all the powers, and duties of the governing body which has been superseded;
  - (c) All such property of the recognized Health Information Exchange as the person or persons appointed under sub-section (2) may, by order in writing, specify in this behalf as being necessary for the purpose of enabling him or them to carry on the business of the Health Information Exchange, shall vest in such persons.
- (4) The National Digital Health Authority of India may at time before the determination of the period of office of any person or persons appointed under this section call upon the recognized Health Information Exchange to re-constitute the governing body in accordance with its rules and on such re-constitution all the property of the recognized Health Information Exchange which has vested in, or was in the possession of the person or persons appointed under sub-section (2), shall revert or vest as the case may be, in the governing body so re-constituted.

**Provided** that until a governing body is so re-constituted, the person or persons appointed

under sub-section (2), shall continue to exercise and perform their powers and duties.

## **CHAPTER V**

### **DIGITAL HEALTH CARE DATA BREACH AND CONSEQUENCES**

---

#### **39. THE BREACH OF DIGITAL HEALTH CARE DATA**

- (1) The digital health care data under this Act is said to be breached, if,
  - (a) The Health Service Provider and the Health Information Exchanges does any act which is in contravention of this Act; or
  - (b) If digital health care data is not stored or transmitted by any Health Information Exchange or Health Service Provider as per the norms under this Act or the standards laid down by National Digital Health Authority of India; or
  - (c) Any person or entity(s) inadvertently does any act which is in contravention with this Act; or
  - (d) Any person or entity(s) does anything which is in contravention with the exclusive right conferred upon the owner of the digital health care data; or

- (e) Any person or entity(s) un-authorizingly procures, stores or transmits the digital health care data; or
  - (f) Any person or entity(s) un-authorizingly use the digital health care data for the purposes other than mentioned under this Act; or
  - (g) Any person or entity(s) un-authorizingly uses the digital health care data for the Commercial Purposes/ Commercial gain; or
  - (h) Any person or entity(s) causes any damage, destroys or deletes or affects it injuriously by any means or tampers any digital health care data existing in any digital form.
- (2) For the purposes of this Act, the Serious Digital Health Care Data Breach shall be, if,
- (a) The digital health care data breach of similar nature pertaining to the same individual for the second or repeated times; or
  - (b) Potential number of individuals are affected; or
  - (c) Involving serious digital health care data or other information of sensitive nature; or

- (d) Whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference; or
  - (e) Vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted; or
  - (f) It involves deliberate or reckless conduct.
- (3) Entities having data where breach has occurred should notify National Digital Health Authority of India and also individual, as the case may be.

#### **40. PENALTIES**

- (1) Any person or entity or entities who contravene the provisions of sub-section (1) of section 39 shall be punished with simple imprisonment for a term which shall extend up to two years and fine which shall be not less than one lakh rupees; or both.
- (2) Any person or entity or entities who contravene the provisions of sub-section (2) of Section 39 shall be punished with simple imprisonment which shall extend from two years and up to four years; and fine which shall not be less than five lakh of rupees.
- (3) Provided that, without prejudice to anything stated elsewhere, any fine imposed as part of

sub-section (2) of this section may be provided to the individual by the Court, as it deems fit as compensation.

#### **41. PENALTY FOR FAILURE TO FURNISH INFORMATION, RETURN etc.,**

Any person or Health Information Exchange, which is required under this Act or any rules made thereunder to furnish any information or document or books or returns or reports etc., to National Digital Health Authority of India or such other Designated Authority, by Central Government, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues;

#### **42. COGNIZANCE OF OFFENCES BY COURT**

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations or bye-laws made thereunder, save on complaint made by the Central Government or State Government or the National Digital Health Authority of India or such designated authority by the Central Government.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under this Act.

### 43. OFFENCES BY COMPANIES

- (1) Where an offence under this Act has been committed by a company or such other incorporated body, every person who, at the time when the offence was committed, was in charge of, and/or was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence, and shall be liable to be proceeded against and punished accordingly.

**Provided** that nothing contained in this subsection shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence.

- (2) Notwithstanding anything contained in subsection (1) above, where an offence under this Act has been committed by a Company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any gross negligence on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall

also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(3) **Explanation** – For the purpose of this Section –

(a) **“Company”** shall mean anybody corporate and includes a firm or other association of individuals; and

(b) **“Director”** in relation to

(i) a firm, means a partner in the firm;

(ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;

(4) The provisions of this section shall be in addition to, and not in derogation of other provisions of this Act.

## **CHAPTER VI**

### **ADJUDICATING AUTHORITY AND APPELLATE AUTHORITY**

---

#### **44. PERSON COMPLAINING TO ADJUDICATING AUTHORITY**

- (1) For any data breach an aggrieved person or owner may complain to the Adjudicatory Authority in writing as may be prescribed by Central Government, and seek reasonable monetary compensation (damages) for the digital health care data breach and consequence thereof.
- (2) No such complaint shall be made after two years from the date of, such person or owner coming to know about the digital health care data breach.
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification.
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time.



#### **45.ADJUDICATING AUTHORITIES, COMPOSITION, POWERS ETC.**

- (1) The Central Government shall by Notification, appoint an Adjudicating Authority or such number of Adjudicating Authorities, depending upon the local requirements, to exercise jurisdiction, powers and authority conferred by or under this Act.
- (2) An Adjudicating Authority shall consist of a Chairperson and two other members, provided that at least one of such person shall be from the field of law.
- (3) A person shall, however, not be qualified for appointment as Members of an Adjudicating Authority –
  - (a) In the field of law, unless he
    - (i)Is qualified for appointment as District Judge; or
    - (ii)Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
  - (b) In the field of medicine, information (health) science or administration unless he possesses such qualifications as may be prescribed by the Central Government.

- (4) The Central Government shall appoint a Member to be the Chairperson of the Adjudicating Authority.
- (5) Subject to the provisions of this Act,
  - (a) The jurisdiction of the Adjudicating Authority may be exercised by the Benches thereof;
  - (b) A Bench may be constituted by the Chairperson of the Adjudicating Authority may be exercised by Benches thereof;
  - (c) A Bench may be constituted by the Chairperson of the Adjudicating Authority with one or two Members as the Chairperson of the Adjudicating Authority may deem fit;
  - (d) The Benches of the Adjudicating Authority shall ordinarily sit at the State Capitals; and such other places as the Central Government may, in consultation with the Chairperson by notification, specify;
  - (e) The Central Government shall, by notification, specify the areas in relation to which each Bench of the Adjudicating Authority may exercise jurisdiction.
- (6) Notwithstanding anything contained in sub-section (5), the Chairperson may transfer a Member from one Bench to another Bench.

- (7) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member that the case or matter is of such a nature that it ought to be heard by a Bench consisting of two Members, the case or matter may be transferred by the Chairperson or, as the case may be, referred to him for transfer, to such Bench as the Chairperson may deem fit.
- (8) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.
- Provided** that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.
- (9) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed by the Central Government.
- Provided** that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.
- (10) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government shall appoint another person in accordance with the provisions of this

Act to fill the vacancy and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.

- (11) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government, resign his office:

**Provided** that, the Chairperson or any other Member shall, unless he is permitted by the Central Government or relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (12) The Chairperson or any other Members shall not be removed from his office except by an order made by the Central Government after giving necessary opportunity of hearing.
- (13) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in

accordance with the provisions of this act to fill such vacancy, enters upon his office.

- (14) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (15) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

#### **46. STAFF OF THE ADJUDICATING AUTHORITY**

- (1) The Central Government shall provide each Adjudicating Authority with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees

of the Adjudicating Authority shall be such as may be prescribed by the Central Government.

#### **47. POWER REGARDING SUMMONS, PRODUCTION OF DOCUMENTS AND EVIDENCE**

- (1) The Adjudicating Authority shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely
  - (a) Discovery and inspection;
  - (b) Enforcing the attendance of any person, including any officer of a Health Service Provider or a Health Information Exchange and examining him on oath;
  - (c) Compelling the production of records;
  - (d) Receiving evidence on affidavits;
  - (e) Issuing commissions for examination of witnesses and documents; and
  - (f) Any other matter which may be prescribed by the Central Government.
- (2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or

make statements, and produce such documents as may be required.

- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

#### **48. ESTABLISHMENT OF APPELLATE TRIBUNAL**

The Central Government shall, by Notification, establish an Appellate Tribunal to hear appeals against the orders of the Adjudicating authority and authorities under this Act.

#### **49. APPEALS TO APPELLATE TRIBUNAL**

- (1) Save as otherwise provided in sub-section (2) below, any person aggrieved by an order made by the Adjudicating Authority under this Act, may prefer an appeal to the Appellate Tribunal.
- (2) Every appeal preferred under sub-section (1) above shall be filed within a period of forty-five days from the date on which a copy of the order made by the Adjudicating Authority is received and it shall be in such form and be accompanied by such fee as may be prescribed by the Central Government.

**Provided** that the Appellate Tribunal may after giving an opportunity of being heard entertain an appeal after the expiry of the said period of forty-five days, if it is satisfied that there was

sufficient cause for not filing it within that period.

- (3) On receipt of an appeal under sub-section (1) above, the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming or modifying or setting aside the order appealed against.
- (4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Adjudicating Authority.
- (5) The appeal filed before the Appellate Tribunal under sub-section (1) or sub-section (2) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within three months from the date of filing of the appeal.

#### **50.COMPOSITION ETC., OF THE APPELLATE TRIBUNAL**

- (1) The Appellate Tribunal shall consist of a Chairperson and two other Members.
- (2) Subject to the provisions of this Act.
  - (a) The jurisdiction of the Appellate Tribunal may be exercised by the Benches thereof;



- (b) A Bench may be constituted by the Chairperson with one or two Members as the Chairperson may deem fit;
  - (c) The Benches of the Appellate Tribunal shall ordinarily sit at New Delhi and such other places as the Central Government may, in consultation with the Chairperson, by Notification, specify.
  - (d) The Central Government shall, by Notification, specify the areas in relation to which each Bench of the Appellate Tribunal may exercise jurisdiction.
- (3) Notwithstanding anything contained in sub-section (2), the Chairperson may transfer a Member from one Bench to another Bench.
- (4) If at any stage of hearing of any case or matter it appears to the Chairperson or a Member that the case or matter is of such a nature that it ought to be heard by a Bench consisting of two Members, the case or matter may be transferred by the Chairperson or, as the case may be referred to him for transfer, to such Bench as the Chairperson may deem fit.

## **51. QUALIFICATIONS FOR APPOINTMENT**

- (1) A person shall not be qualified for appointment as Chairperson unless he is or has been Judge of Supreme Court or of a High Court or is qualified to be a Judge of the High Court.
- (2) A person shall not be qualified for appointment as a Member unless he
  - (a) Has been a Member of the Indian Legal Service and has held a post in Grade I of that Service for at least three years; or
  - (b) Has been rendered at least ten years of service in Central Medical Services; or
  - (c) Such other relevant qualification to be prescribed by the Central Government.
- (3) No sitting Judge of the Supreme Court or of a High Court shall be appointed under this section except after consultation with the Chief Justice of India.
- (4) The Chairperson or a Member holding a post as such in any other Tribunal, established under any law for the time being in force, in addition to his being the Chairperson or a Member of that Tribunal, may be appointed as the Chairperson or a Member, as the case may be, of the Appellate Tribunal under this Act.

## 52. TERM OF OFFICE

The Chairperson and every other Member shall hold office as such for a term of five years from the date on which he enters upon his office.

**Provided** that no Chairperson or other Member shall hold office as such after he has attained

- (a) In case of the Chairperson, the age of sixty-eight years;
- (b) In the case of any other member, the age of sixty-five years.

## 53. CONDITIONS OF SERVICE

The salary and allowances payable to and the other terms and conditions of service (including tenure of office) of the Chairperson and other Members shall be such as may be prescribed.

**Provided** that, neither the salary and allowance nor the other terms and conditions of service of the Chairperson or any other Members shall be varied to his disadvantage after appointment.

## 54. VACANCIES

If, for reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government shall appoint another person in accordance with the provisions of this act to fill the vacancy and the

proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.

## **55. RESIGNATION AND REMOVAL**

- (1) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government, resign from his office;

**Provided** that the Chairperson or any other Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whoever is the earliest.

- (2) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government on the ground of proved misbehavior or incapacity, after an inquiry made by a person appointed by the President in which such Chairperson or any other Member concerned had been informed of the charges against him and given a reasonable opportunity of being heard in respect of those charges.

## **56. MEMBER TO ACT AS CHAIRPERSON IN CERTAIN CIRCUMSTANCES**

- (1) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior most Member shall act as the Chairperson until the date on which the new Chairperson, appointed in accordance with the provisions of this Act to fill such vacancy, enters upon his office.
- (2) When the Chairperson is unable to discharge his functions owing to absence, illness or any other cause, the senior most Member shall discharge the functions of the Chairperson until the date on which the Chairperson resumes his duties.

## **57. STAFF OF THE APPELLATE TRIBUNAL**

- (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may think fit.
- (2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of the Chairperson
- (3) The salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal shall be such as may be prescribed by the Central Government.

## **58. PROCEDURE AND POWERS OF APPELLATE TRIBUNAL**

- (1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.
- (2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint.
- (3) An order made by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court and, for this purpose the Appellate Tribunal shall have all the powers of the Civil Court.
- (4) Notwithstanding anything contained in sub-section (3) above, the Appellate Tribunal may transmit any order made by it to the Civil Court having local jurisdiction and such Civil Court shall execute the order as if it were a decree made by that court.
- (5) All the proceedings before the Appellate Tribunal shall be deemed to be judicial

proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 (45 of 1860) and the Appellate Tribunal shall be deemed to be a Civil Court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

#### **59. DISTRIBUTION OF BUSINESS AMONG BENCHES**

Where any Benches are constituted, the Chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the Benches and also provide for the matters which may be dealt with by each Bench.

#### **60. POWER OF THE CHAIRMAN TO TRANSFER CASES**

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may desire to be heard, or on his own motion without such notice, the Chairperson may transfer any case pending before one Bench, for disposal, to any other Bench.

#### **61. DECISION TO BE BY MAJORITY**

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson who shall either hear the point or points himself or refer the case for hearing on such point or points by third Member of the Appellate

Tribunal and such point or points shall be decided according to the opinion of the majority of the Members of the Appellate Tribunal who have heard the case, including those who first heard it.

## **62. MEMBERS ETC., TO BE PUBLIC SERVANTS**

The Chairperson, Members and other officers and employees of the Appellate Tribunal, the Adjudicating Authority and the officers subordinate to it shall be deemed to be public servants within the meaning of Section 21 of the Indian Penal Code, 1860 (45 of 1860).

## **63. CIVIL COURT NOT TO HAVE JURISDICTION**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Authority or the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

## **64. APPEAL TO HIGH COURT**

- (1) Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of law or fact arising out of such order.



- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

## **CHAPTER VII**

### **MISCELLANEOUS PROVISIONS**

---

#### **65. POWER OF THE CENTRAL GOVERNMENT TO MAKE RULES**

The Central Government may, by notification, make rules for the purposes of carrying out the provisions of this Act.

#### **66. REMOVAL OF DIFFICULTY BY THE GOVERNMENT**

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of

this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.

- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

**67. DIGITAL HEALTH CARE DATA TO BE USED FOR  
RESEARCH, ACADEMIC AND SUCH OTHER  
RELATED PURPOSES**

- (1) The Health Service Providers or Health Information Exchanges are compelled under this Act to maintain the anonymity of digital health care data to be transferred for the research, academic and such other related purposes.

Such digital health care data transferred for research, academic and such other related purposes shall be used anonymously as prescribed by National Digital Health Authority of India.

\* \* \* \* \*

## Digital Healthcare Data Privacy, Confidentiality & Security Act

### Executive Summary

The main objective of the draft **Digital Healthcare Data Privacy, Confidentiality & Security Act** is to ensure the improvement of the quality of health services in the country, through the use of digital information technology, which will make the provision of health services more efficient, cost effective and transparent. In the same vein, the Act puts equal emphasis, on the protection of confidential medical information.

Presently, a patient who accesses medical services is unlikely to be able to provide a health care provider with their complete medical history, unless they carry their complete records, diligently maintained. Further, a patient is required to undergo a number of different diagnostic tests, based on which health care services are provided. If the patient accesses health services subsequently, even at the same health care setting, the service provider is likely to be different. Similarly, they may seek health services at an altogether different health care setting. The diagnostic tests are likely to be repeated, which is expensive, inefficient and time consuming. At the same time, a large number of private health service providers have adopted digital systems of storing health information of a patient. These, however, are without any standards and with inadequate data security measures.

In the context set out above, this Act seeks to provide for the digitisation of the health information of a person, and regulate its collection, storage and access as well as provide for strong data security measures to protect the confidentiality of digital health data. The key features of the draft Act are as follows:

- 1. Establishment of National Authority and State Authorities:** The Act seeks to create a National Digital Health Authority of India, headed by a Chairperson and having nine other members. The National Authority is required to lay down standards for the generation, collection, storage and transmission of digital health care data, as well as ensure that such data is not breached. Similarly, the State Authorities will be created in each state. A state authority must ensure that all entities adopt the standards set by the National Authority.
- 2. Establishment of health information exchanges:** The Act further seeks to establish 'Health Information Exchanges' (HIEs), which will be done by the Central Government. HIEs are required to store digital health care data and provide access to clinical establishments, in accordance with the provisions of the Act. The HIEs are subject to the directions of the National Authority.
- 3. Distinction in the nature of data:** As health care information is sensitive in nature, the Act seeks to define different levels of data and restrict access accordingly. Under

the Act, digital health care data is an electronic record of a person's health information and may include services accessed by them, results of diagnostic tests, courses of treatment taken and particulars of medical establishments that were accessed. Further, personally identifiable data has been defined, which may be used only for the limited purpose of direct treatment and care of the person concerned. Personally identifiable data would include any information, which could lead to the identification of the person and would include their name, address, physical and mental health, sexual orientation and biometric information, amongst others.

Data may also be anonymised for certain purposes, which would entail the permanent deletion of all personally identifiable data. It may also be de-identified for certain purposes, which entails a process of obscuring personally identifiable data, in a manner which could allow it to be linked again, if necessary.

4. **Restricted purposes:** The Act seeks to ensure that digital health care data may only be collected, stored, transmitted or used for the purposes of the Act and no other. To this end, personally identifiable data may only be used to advance the delivery of patient centered medical care; to provide appropriate information to guide medical a case; and to improve coordination of care amongst hospitals. De-identified or anonymised data may be used to improve public health facilities; to promote public health; promote early detection of disease; and to undertake academic research, amongst others. No information may be used for commercial purposes.
5. **Protection of the rights of owners:** The Act seeks to protect the rights of owners of digital health care data. It sets out that the right to privacy, confidentiality and security of digital health care data will be secured under the Act. The right to consent for the generation and collection of digital health care data as well as to subsequently withdraw consent for storage has been provided for. The owner also has the right to know which clinical establishment has accessed their data, and should be notified, if there is a data breach.
6. **Collection, storage and transmission of digital health care data:** A clinical establishment, defined under the Act, may collect and generate the digital health care data of a person, only with their consent. The consent for collection of digital health care data cannot be made mandatory for the provision of health services.

Digital health care information may be securely transmitted to an HIE, with the consent of the owner of the information. The clinical establishment may retain a copy of the information for its own reasonable use.

Both the HIEs and the clinical establishments storing the data must adhere to data protection norms prescribed by the National Authority, ensuring the privacy and confidentiality of the owner.

7. **Access to digital health care data:** Under the Act, a clinical establishment may access the digital health information of an owner from an HIE only on a need to know basis. This means that information can only be accessed for a specific and lawful purpose and only that information which is necessary to carry out that function need be accessed. This is modeled on the concept of shared confidentiality in common law, where confidential information may be shared between doctors, nurses and other service providers for the treatment of a person.
8. **Breach and serious breach of digital health care data:** The collection, storage, transmission or disclosure of digital health care information contrary to the provisions of the Act will be considered a breach, which entitles the person to claim damages by way of compensation. Aggravated breaches or breaches accompanied by criminal intention (*mens rea*) are treated as serious breaches, which are treated as criminal offences. Other criminal offences have also been defined, including data theft, obtaining the digital health information of another and failure to furnish information and file returns.
9. **Remedies for breach and serious breaches:** A complaint about a breach of information may be made to an Adjudicating Authority, established under the Act. For a breach by a clinical establishment, a State Adjudicating Authority ought to be approached. For a breach by a HIE, the National Authority or a State Authority, the Central Adjudicating authority may be approached. The Central Adjudicating Authority will be appointed by the Central Government and the State Authorities by the respective State Governments. They will each consist of three members and reflect an expertise of law and technical knowledge. An order of an adjudicating authority may be appealed to a High Court.

For a serious breach, a criminal complaint may be filed in a Sessions Court.

# **Digital Healthcare Data Privacy, Confidentiality & Security Act**

***[Draft for Public Consultation]***

**September, 2017**

**Ministry of Health & Family Welfare,  
Government of India**

**INDEX**

<b>SL. NO.</b>	<b>PARTICULARS</b>	<b>PAGE NO.</b>
1	CHAPTER I – PRELIMINARY	2
2	CHAPTER II - NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA  STATE DIGITAL HEALTH AUTHORITIES  HEALTH INFORMATION EXCHANGES	6
3	CHAPTER III – POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES	13
4	CHAPTER IV - DATA OWNERSHIP, SECURITY AND STANDARDIZATION	
5	CHAPTER V- DIGITAL HEALTH DATA BREACH AND CONSEQUENCES	24
6	CHAPTER VI- ADJUDICATING AUTHORITY	27
7	CHAPTER VII- MISCELLANEOUS PROVISIONS	31



**Digital Healthcare Data Privacy, Confidentiality & Security Act, (INSERT YEAR)**

*An Act to provide for establishment of National and State Digital Health Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data and such other matters related and incidental thereto.*

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

**CHAPTER I  
PRELIMINARY****1. SHORT TITLE, EXTENT**

- (1) This Act may be called as Digital Healthcare Data Privacy, Confidentiality & Security Act (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

**2. COMMENCEMENT AND APPLICATION**

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.

**3. DEFINITIONS**

- (1) In this Act, unless the context otherwise requires,
  - (a) **'Anonymization'** means the process of permanently deleting all personally identifiable information from an individual's digital health data.
  - (b) **'Breach'** shall have the same meaning as assigned to it in Section 34 of this Act.
  - (c) **'Consent'** means expressed informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.

Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.

- (d) **'De-identification'** means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that

eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.

- (e) **‘Digital Health Data’** means an electronic record of health-related information about an individual and shall include the following:
  - (i) Information concerning the physical or mental health of the individual;
  - (ii) Information concerning any health service provided to the individual;
  - (iii) Information concerning the donation by the individual of any body part or any bodily substance;
  - (iv) Information derived from the testing or examination of a body part or bodily substance of the individual;
  - (v) Information that is collected in the course of providing health services to the individual; or
  - (vi) Information relating to details of the clinical establishment accessed by the individual.
- (f) **‘Entity’** includes any of the following, not being a clinical establishment:
  - (i) An individual;
  - (ii) A company;
  - (iii) A department of the Central or State Government;
  - (iv) A firm;
  - (v) An association of persons or a body of individuals, whether incorporated or not, in India or outside India; or
  - (vi) Any corporation established by or under any Central, State or Provincial Act or a Government company as defined in section 2(45) of the Companies Act, 2013;
  - (vii) Any body corporate incorporated by or under the laws of a country outside India;
  - (viii) A co-operative society registered under any law relating to cooperative societies;
  - (ix) A local authority;
  - (x) Every artificial juridical person, not falling within any of the preceding sub-clauses;
- (g) **‘Guardian’** means a guardian recognised under any law for the time being in force.
- (h) **‘Health Information Exchange’** means a health information exchange as established under this Act.
- (i) **‘Clinical Establishment’** means (i) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution

by whatever name called offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicines established and administered or maintained by any person or body of persons, whether incorporated or not; or (ii) a place established as an independent entity or part of an establishment referred to in sub-clause (i), in connection with the diagnosis where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not, and shall include a clinical establishment owner, controlled or managed by

- a. the Government or a department of the Government;
  - b. a trust, whether public or private;
  - c. a corporation (including a society) registered under a Central, Provincial or State Act, whether or not owned by the Government;
  - d. a local authority;
  - e. a single doctor,
- but does that include the clinical establishments owned, controlled or managed by the Armed Forces.  
Explanation: For the purpose of this clause, “Armed Forces” means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)

- (j) **‘Owner’** means an individual whose digital health data is generated and processed under this Act.
- (k) **‘Personally Identifiable Information’** means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I.
- (l) **‘Prescribed’** shall mean rules prescribed by the Central Government or the State Governments as the case may be.
- (m) **‘Relative’** shall have the same meaning as assigned to it under Clause (u) of section 2 of the Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Act, 2017.

- (n) **‘Data Security’** refers directly to protection of digital health data, and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.
- (o) **‘Sensitive health-related information’** means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, HIV status, STI treatment, and abortion.
- (p) **‘serious breach’** shall have the same meaning as assigned to it in Section 35 of this Act.
- (q) **‘Specified’** shall mean as specified by National Digital Health Authority of India or State Digital Health Authority, as the case may be.
- (r) **“need to know basis”** means the access to digital health data by a specific person for a specific and lawful purpose that is necessary for that purpose or to carry out that function.

CHAPTER II  
NATIONAL DIGITAL HEALTH AUTHORITY OF INDIA,  
STATE DIGITAL HEALTH AUTHORITIES AND  
HEALTH INFORMATION EXCHANGES

**4. National Digital Health Authority of India**

- (1) The Central Government shall establish for the purposes of this act, a National Digital Health Authority of India, by Notification in the Official Gazette, which may be referred to as NDHAI in its abbreviated form.
- (2) The National Digital Health Authority of India, shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government, specifies a separate date in the same Notification.

**5. Composition of National Digital Health Authority of India**

- (1) National Digital Health Authority of India shall consist of the following members, to be appointed by the Central Government by Notification, namely:
  - (a) A full time Chairperson;
  - (b) Joint Secretary, Health, as member-secretary;

- (c) Four full-time members to be appointed by the Central Government:
    - (i) 1 from health informatics;
    - (ii) 1 from public health;
    - (iii) 1 from law; and
    - (iv) 1 from public policy
  - (d) Four ex-officio members, not less than the rank of Joint Secretary to be appointed by the Central Government:
    - (i) 1 from Information Technology;
    - (ii) 1 from Panchayati Raj/Woman & Child Development;
    - (iii) 1 from DGHS; and
    - (iv) 1 from law department
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
  - (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Fifteen years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.

Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building and cause of commitment.
- (3) The Central Government, shall form a Cell to be headed by Joint Secretary, Health supported by Deputy/Assistant Commissioners, consultants and other support staff as required for executing the directions or recommendations of the National Authority and assisting the Authority in carrying out its functions under this Act.  
 Provided that the Cell may, as and when it considers necessary, associate with institutions and experts for the efficient discharge of its functions.
- (4) The National Authority shall be a body corporate with the name specified by the Central Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and dispose of property and to contract, and may, by the said name, sue or be sued.

## 6. State Digital Health Authorities

- (1) Every State Government shall, as soon as may be after the issue of the notification under sub-section (1) of section 4, by notification in the Official Gazette, establish a State Digital Health Authority, which may be referred to as SDHA in its abbreviated form.

- (2) The State Digital Health Authority shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the State Government, specifies a separate date in the same Notification.

## **7. Composition of State Digital Health Authorities**

- (1) State Digital Health Authority shall consist of the following members, to be appointed by the State Government by Notification, namely:
- (a) A full time Chairperson;
  - (b) Secretary Health or equivalent as member-secretary;
  - (c) Three full-time members to be appointed by the State Government:
    - (i) 1 from health informatics;
    - (ii) 1 from public health; and
    - (iii) 1 from law
  - (d) Three ex-officio members to be appointed by the State Government:
    - (i) Director, Health Services;
    - (ii) 1 from Information Technology; and
    - (iii) 1 from law department
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
- (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Twelve years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.
- Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building and cause of commitment.
- (3) The State Government, shall form a Cell to be headed by Secretary, Health, supported by Directors/Jt. Directors, consultants and other support staff as required for executing the directions or recommendations of the State Authority and assisting the Authority in carrying out its functions under this Act.
- Provided that the Cell may, as and when it considers necessary, associate with institutions and experts for the efficient discharge of its functions.
- (4) The State Authority shall be a body corporate with the name specified by the State Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and dispose of property and to contract, and may, by the said name, sue or be sued.

**8. Term of Office of Chairperson & other members of National and State Authorities**

- (1) The Chairperson and other members of the National Authority, shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (2) The chairperson and other members of the State Authority, shall hold office for a term of three years, as the State Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (3) The Chairperson and other Members, appointed as per sub-section (1) of section 5 and sub-section (1) of section 7, are eligible for reappointment for another term or such other terms as the case may be; provided such reappointed Chairperson or Member does not exceed sixty-five years of age.

**9. Salary, allowance, benefits and service conditions etc.,**

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members, of the National Authority may be prescribed by the Central and State Governments respectively.
- (2) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members, of the State Authorities, shall be such as may be prescribed by the State Governments respectively.
- (3) Notwithstanding anything stated in sub-section (1) and (2) above, the salary, allowances and other conditions of service of the Chairperson or of a member shall not be varied to his disadvantage after his appointment.

**10. Reconstitution of the National and State Authorities**

- (1) Any vacancy caused to the office of the Chairperson or any other member of the National Authority shall be filled up by the Central Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (2) Any vacancy caused to the office of the Chairperson or any other member of the State Authority shall be filled up by the State Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (3) In the event of vacancy in the office of the Chairperson of the National or State Authority, the senior most person, from amongst the full time members, shall act as the Chairperson, till the vacancy is filled.
- (4) No act or proceeding of the National or State Authority shall be invalid merely by reason of-
  - (a) Any vacancy in, or any defect in the constitution of the Authority; or

- (b) Any defect in the appointment of a person acting as a member of the Authority; or
- (c) Any irregularity in the procedure of the Authority not affecting the merits of the case.

**11. Temporary association of persons with National or State Authorities for particular purposes –**

- (1) The National Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (2) A State Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (3) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall have a right to take part in the discussions of the Authority relevant to that purpose, but shall not have a right to vote at a meeting of the Authority, and shall not be a member for any other purpose.
- (4) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall be paid such fees and allowances, for attending its meetings and for attending to any other work of the Authority, as may be prescribed.

**12. Officers and Other Employees of the National and State Authorities**

- (1) The National Authority, in consultation with Central Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (2) The State Authority, in consultation with the State Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (3) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the National or State Authority appointed under sub-section (1) and (2) shall be such as may be prescribed.

**13. Meetings**

- (1) The National Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be provided by regulations.
- (2) The State Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be provided by regulations.



- (3) The chairperson of the National or State Authority, if unable to attend a meeting, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

#### **14. Disqualifications**

- (1) A person shall be disqualified for appointment as Chairperson or member of the National Digital Health Authority or a State Digital Health Authority, if he/she –
  - (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (ii) Is an undercharged insolvent; or
  - (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
  - (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
  - (v) Has such other disqualification as may be prescribed by the Central Government.

#### **15. Resignation, removal of chairperson or member of the National or State Authorities**

- (1) The Chairperson or full time member of the National Authority appointed under sub-section (1) of section 5 and the Chairperson or full time member of a State Authority appointed under sub-section (1) of section 7:
  - (a) May relinquish his/her office by submitting the resignation in writing to the Central Government or the State Government as the case may be; or
  - (b) May be removed from his/her office in accordance with the provisions of section 16.

#### **16. Removal in certain circumstances**

- (1) The Central Government or the State Government, may remove from office the Chairperson or any full-time member of the National or State Authority, who –
  - (a) Has been adjudged as an insolvent; or
  - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (c) Has become physically or mentally incapable of discharging his or her functions; or
  - (d) Has acquired such financial or other interest as is likely to affect prejudicially his or her functions as the Chairman or member; or
  - (e) Has so abused his/her position as to render his or her continuance in office prejudicial to the public interest.

- (2) No such member or Chairperson shall be removed from his/her office under clause (d) or clause (e) of sub-section (1) above, unless he/she has been given a reasonable opportunity of being heard in the matter.

#### **17. Health Information Exchanges**

- (1) The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act
- (2) No entity shall function as a Health Information Exchange unless established as such by the central Government

#### **18. Management of Health Information Exchange**

- (1) All Health Information Exchanges shall conduct and carry out their affairs strictly as per the norms, standards or protocols prescribed by the National Digital Health Authority of India from time to time or as per the Rules prescribed by the Central Government.
- (2) Without prejudice to any other stipulations of this Act, a Health Information Exchange established under section 17 shall only employ such skilled personnel for management of its affairs as may be specified by the National Digital Health Authority of India.
- (3) Conditions with respect to periodical reports, annual reports and direct inquiries may be such as may be prescribed.

#### **19. The Chief Health Information Executive and his functions**

- (1) The Health Information Exchange shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the National Digital Health Authority of India.
- (2) The Chief Health Information Executive as appointed under sub-section (3) above, shall be the Chief Executive Officer and also the data controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs, and in particular:
  - (a) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
  - (b) Access, and process the digital health care data transmitted by the Clinical Establishments to further transmit the digital health care data, whenever required, in accordance with norms prescribed by the National Digital Health Authority of India.
  - (c) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
  - (d) Notify the data breach to the owner and such other concerned.
  - (e) Store the digital health care data in prescribed mode in all situations.

CHAPTER III  
POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES

**20. Powers and functions of National Digital Health Authority of India**

- (1) The National Digital Health Authority of India in order to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Formulate standards, operational guidelines and protocols for the generation, collection, storage and transmission of the digital health data for the purposes of this Act, applicable to:
    - (i) Clinical establishments generating and collecting digital health data for their own use or for further transmission to the health information exchanges;
    - (ii) Health information exchanges storing and transmitting digital health data to clinical establishments, or other health information exchanges, or to State Digital Health Authority, or the National Digital Health Authority;
    - (iii) Any other entity having custody of any digital health data;
    - (iv) State Digital health Authority and the National Digital Health Authority;
  - (b) To ensure data protection and prevent breach or theft of digital health data, establish data security measures for all stages of generation, collection, storage and transmission of digital health data, which shall at the minimum include access controls, encrypting and audit trails;
  - (c) Conduct periodical investigations to ensure compliance with the provisions of this Act and any rules, regulations, standards or protocols hereunder by health information exchanges;
  - (d) Notify and mandate the health information exchanges, in case of failure to comply with the provisions of this Act;
  - (e) To lay down protocol for transmission of digital health data abroad and for receiving it from abroad;
  - (f) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
  - (g) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed

**21. National Authority's power of oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 20, the National Digital Health Authority of India or its representative, shall have the right to inspect all such records; or access the premises, including virtual premises of the health information exchange or exchanges at any time.

**Provided** that National Digital Health Authority of India while accessing such records or accessing either the physical or virtual premises of health information exchanges, shall bear in mind that no or least possible hindrance is caused to the normal working of the health information exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Digital Health Authority of India to generally discharge its functions under this Act, shall direct a health information exchange or class of health information exchanges, or all health information exchanges as the case may be, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the National Digital Health Authority of India shall be binding upon the health information exchange or health information exchanges.

**22. Powers and Functions of State Digital Health Authorities**

- (1) The State Digital Health Authority to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Ensure that the clinical establishments and other entities in the state collect, store, transmit and use digital health data as per the provisions of this Act and the standards, protocols and operational guidelines issued by the National Digital Health Authority, from time to time;
  - (b) Conduct investigations to ensure compliance with the provisions of this Act;
  - (c) Notify and mandate the clinical establishments and other entities, in case of failure to comply with the provisions of this Act;
  - (d) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (c) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed

**23. State Authority's power of Oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the State Digital Health Authority, or its representative,

shall have the right to inspect all such records; or access the premises including virtual premises, of a Clinical establishment or entities at any time.

**Provided** that State Digital Health Authority while accessing such records or accessing the physical premises of Clinical establishments, shall bear in mind that no or least possible hindrance is caused to the normal working of the clinical establishment

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the State Digital Health Authority to generally discharge its functions under this Act, it shall direct a clinical establishment or a class of clinical establishments, or all clinical establishments as the case may be, or entities, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the State Digital Health Authority are binding upon the clinical establishment or clinical establishments and entities as the case may be.

**24. Power of Civil Court** – Notwithstanding anything contained in any other law for the time being in force, the National Authority while exercising the powers under section 21 and the State Authorities while exercising the powers under section 23, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-

- (a) summoning and enforcing the attendance of witnesses and examining them on oath;
- (b) discovery and production of any document;
- (c) receiving evidence on affidavit;
- (d) requisitioning any public record or copy thereof from any court or office;
- (e) issuing commissions for examination of witnesses or documents;
- (f) any other matter which may be prescribed

**25. Power to give directions –**

- (1) In the performance of its functions under this Act, -
  - (a) The National Authority shall be bound by such directions in writing as the Central Government may give to it;
  - (b) Every State Authority shall be bound by such direction in writing as the National Authority or the State Government may give to it; *Provided that* where a direction given by the State Government is inconsistent with the direction given by the National Authority, the matter shall be referred to the Central Government for its decision, which shall be final.
  - (c) Every Health Information Exchange shall be bound by such directions in writing as the National Authority may give to it;
  - (d) Every Clinical Establishment shall be bound by such directions in writing as the State Authority may give to it.

**CHAPTER IV**  
**DATA OWNERSHIP, SECURITY AND STANDARDIZATION**

**26. The rights of the owner of digital health data**

- (1) An owner shall have the right to privacy, confidentiality, and security of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.
- (2) An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 27 of this Act.
- (3) An owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data.
- (4) An owner shall have the right to refuse consent to the access or disclosure of his or her digital health data, and if refused it shall not be disclosed, subject to the exceptions provided in Section 31 of the Act.
- (5) An owner of the digital health data shall have the right that the digital health data collected must be specific, relevant and not excessive in relation to the purpose or purposes for which it is sought;
- (6) An owner of the digital health data shall have the right to know the clinical establishments or entities which may have or has access to the digital health data, and the recipients to whom the data is transmitted or disclosed;
- (7) The owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any Clinical Establishment/Entity;
- (8) The owner of the digital health data shall have, subject to sub-section (1) to (3) above:
  - (a) The right to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data, in the prescribed form as may be notified by the National Digital Health Authority;
  - (b) The right to require their explicit prior permission for each instance of transmission or use of their digital health data in an identifiable form, through such means as may be prescribed;
  - (c) The right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 32 of the Act;
  - (d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;

- (e) The right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner;
- (f) The right not to be refused health service, if they refuse to consent to generation, collection, storage, transmission and disclosure of their health data;
- (g) The right to seek compensation for damages caused by a breach of digital health data.

**27. Purposes of collection, storage, transmission and use of the digital health data**

- (1) Digital health data may be generated, collected, stored, and transmitted by a clinical establishment, and stored and transmitted by health information exchange, and entities for the following purposes:
  - (a) To advance the delivery of patient centered medical care;
  - (b) To provide appropriate information to help guide medical decisions at the time and place of treatment;
  - (c) To improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;
  - (d) To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;
  - (e) To facilitate health and clinical research and health care quality;
  - (f) To promote early detection, prevention, and management of chronic diseases;
  - (g) To carry out public health research, review and analysis, and policy formulation;
  - (h) To undertake academic research and other related purposes

Provided that personally identifiable information may only be used for the purposes of direct care of the owner of the data, as specified in clauses (a) to (c) of sub-section (1), subject to provisions of section 25, to the extent considered necessary and in the best interest of the owner

Provided further that for public health related purposes mentioned in clauses (d) to (h) of sub-section (1), only de-identified or anonymized data shall be used, in the manner as may be prescribed under this Act.

- (2) Digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (c) of Sub-Section (1).
- (3) Digital health data shall not be used for any other purpose, except in accordance with the provisions of this Act.

Provided that the digital health data shall be used only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to use the information.

- (4) There shall be no access to, or disclosure of personally identifiable information, except in accordance with the provisions of this Act.

Provided that the digital health data shall be accessed or disclosed only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to access or disclose the information.

- (5) Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the government.

Explanation: Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim.

Provided that for the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates

## **28. Collection of health data**

- (1) No health data shall be collected, for the purposes of conversion to digital health data, by any clinical establishment, or any other entity in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may, by consent from the owner, recorded in the form and manner as may be prescribed under this Act, lawfully collect the required health data, as per the regulations prescribed by the National Digital Health Authority of India, after informing the owner of the following:
  - (a) The rights of the owner as laid down in this Act, including the right to refusal to give consent to the generation and collection of such data;
  - (b) The purpose of collection of such health data;
  - (c) The identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format;
  - (d) The identity of the recipients who may have access to such digital health data on a need to know basis



- (3) A clinical establishment or any other entity, shall furnish a copy of the consent form to the owner.
- (4) Any other entity that collects any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data.
- (5) Without prejudice to the above sub-section (2), when an individual is incapacitated or incompetent to provide consent, either due to physical or mental incapacity, the clinical establishment may collect health data by obtaining proxy consent from a nominated representative, relative, care giver or such other person, as may be prescribed under this Act, and who has the legal capacity to consent.

Provided that where the individual has regained his or her capacity to give or refuse consent for the collection of his or her health data by the clinical establishment, he or she shall have the option to seek withdrawal of proxy consent and obtaining his or her own consent for collection of such health data, in such form and manner as may be prescribed by the National Digital Health Authority of India.

- (6) Where a person is a minor and it is in the best interest of the minor, proxy consent can be obtained by the minor's legal guardian, or representative.

Provided that upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.

## **29. Ownership of digital health data**

- (1) The digital health data generated, collected, stored or transmitted shall be owned by the individual whose health data has been digitised;
- (2) A clinical establishment or Health Information Exchange shall hold such digital health care data referred to in sub-section (1) above in trust for the owner;
- (3) Any other entity who is in custody of any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data;
- (4) Notwithstanding anything stated in the above sub-sections (1) to (3), the medium of storage and transmission of digital health data shall be owned by the clinical establishment or health information exchange, as the case may be.

## **30. Storing of digital health data**

- (1) No digital health data shall be stored by any clinical establishment or entity or health information exchange in any manner, except in accordance with the provisions of this Act.
- (2) The clinical establishment or health information exchange, as the case may be, shall hold all digital health data, on behalf of National Digital Health Authority of India; and such data be used for such purposes as

stated in Section 26, without compromising the privacy or confidentiality of the owner, and security of such data.

- (3) The digital health data vested with the National Digital Health Authority as per sub-section 2 above, shall be stored and may be transmitted or used in such form and manner as may be prescribed by the National Digital Health Authority.

### 31. Transmission of data

- (1) No digital health data shall be transmitted by a clinical establishment or health information exchange, or any other entity, as the case may be, in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the Clinical establishment.

**Provided** that for such secure, encrypted and instantaneous transmission of digital health data as referred in sub-section (2), the National Digital Health Authority of India shall prescribe appropriate standards for physical, administrative and technical measures, keeping in mind the privacy and confidentiality of the owner, by notification.

- (3) The digital health data shall be transmitted by a clinical establishment or entity or health information exchange only upon the consent of the owner, after being informed of the rights of the owner under Section 25, and the specific purposes of collection of such data under Section 26.
- (4) A health information exchange shall maintain a register in such form and manner as may be prescribed, containing all details of the transmission of the digital health data between a clinical establishment and health information exchange, and between health information exchanges *inter se*.

### 32. Access to digital health data

- (1) No digital health data collected, stored or transmitted by a clinical establishment or health information exchange, as the case may be, shall be accessed by any person, except in accordance with the provisions of this Act.
- (2) The digital health data collected or stored or transmitted by a clinical establishment or health information exchange, as the case may be, may be accessed by the clinical establishment, on a need to know basis, in such form and manner as may be prescribed under this Act.
- (3) The government departments through their respective Secretaries, may submit request for digital health data in de-identified/anonymized form, to the National Digital Health Authority, in the form and manner specified by the Authority, subject to provisions of clauses (d) to (h) of sub-section (1) of section 27 of this act.

Provided that the National Digital Health Authority of India may prescribe any other class of persons who may access digital health data,

which is anonymized, for the purposes stated in clause (d) to (h) of sub-section (1) of section 27 of the Act.

- (4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for administration of justice, such access may be granted to an investigating authority only with the order of the competent court;
- (5) The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Digital Health Authority of India.
- (6) In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified;
- (7) In case of an emergency, the relatives of the owner may have access to such data for the purpose of correct treatment of the owner, subject to such conditions as may be prescribed under this Act.
- (8) In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Digital Health Authority of India.

Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.

Provided further that in case of death of the owner, the National Digital Health Authority of India shall use the digital health data only in anonymized form.

- (9) All clinical establishments and health information exchanges shall maintain a register in a digital form to record the purposes and usage of digital health data accessed within the meaning of this Section, in such form and manner, as may be specified by the National Digital Health Authority of India.

### **33. Duty to maintain privacy and confidentiality of digital health data**

- (1) A clinical establishment, health information exchange, State Digital Health Authority and the National Digital Health Authority of India, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner;
- (2) Any other entity, which has generated and collected digital health data, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner.
- (3) The privacy, confidentiality and security of digital health data shall be ensured by taking all necessary physical, administrative and technical measures, that may be prescribed or specified, to ensure that the digital health data, collected, stored and transmitted by them, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.

- (4) Without prejudice to the above provisions, a clinical establishment or health information exchange shall ensure through regular training and oversight that their personnel comply with the security protocols and procedures as may be prescribed or specified under this act.
- (5) A clinical establishment, or a health information exchange, shall provide notice immediately, and in all circumstances not later than three working days to the owner, in such manner as may be prescribed under this Act, in case of any breach or serious breach of such digital health data.

#### **34. Procedure for rectification of digital health data**

- (1) An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed under this Act.
- (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.

### CHAPTER V OFFENCES AND PENALTIES

#### **35. Breach of digital health data**

- (1) Digital health data is said to be breached, if:
  - (a) any person generates, collects, stores, transmits or discloses digital health information in contravention to the provisions of Chapter II of this Act; or
  - (b) Any person does anything in contravention of the exclusive right conferred upon the owner of the digital health data; or
  - (c) Digital health data collected, stored or transmitted by any person is not secured as per the standards prescribed by the Act or any rules thereunder; or
  - (d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data.
- (2) Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place.

#### **36. Serious breach of digital health data:**

- (1) A serious digital health data breach shall be said to have taken place, if:
  - (a) A person commits a breach of digital health data intentionally, dishonestly, fraudulently or negligently; or

- (b) Any breach of digital health data occurs, which relates to information which is not anonymised or de-identified; or
- (c) A breach of digital health data occurs where a person failed to secure the data as per the standards prescribed by the Act or any rules thereunder; or
- (d) Any person uses the digital health data for commercial purposes or commercial gain; or
- (e) An entity, clinical establishment or health information exchange commits breach of digital health data repeatedly;

Explanation: The terms “dishonestly” and “fraudulently” shall have the same meaning as assigned to them under the Indian Penal Code, 1860

- (2) Any person who commits a serious breach of health care data shall be punished with imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.

Provided that, any fine imposed as part of sub-section (2) of section 36 may be provided to the individual whose data is breached, by the Court, as it deems fit as compensation.

### **37. Compensation for serious breach of digital health information**

- (1) A person or an entity committing a serious breach of digital health information shall be liable to pay damages by way of compensation to the owner of the digital health data in relation to which the breach took place.
- (2) Where any compensation has been awarded under sub-section (2) of section 35, it shall be taken into account when determining the claim made by the person affected.

### **38. Penalty for failure to furnish information, return or failure to observe rules and directions, etc.,**

- (1) If any person required under this Act or any rules made thereunder, fails to furnish any information or document or books or returns or reports etc., within the time specified, to National Digital Health Authority of India, or the State Digital Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (2) Any person required under this Act or any rules made thereunder fails to comply, within the time specified, with directions issued by the National Digital Health Authority of India, or the State Digital Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;

- (3) Any person which is required under this Act or any rules made thereunder, after having been called upon by the National Digital Health Authority of India in writing, or the State Digital Health Authority, as the case may be, to redress the grievances of owners of digital healthcare data, fails to redress such grievances within the time specified, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees.

**39. Obtaining the digital health information of another person**

Whoever, fraudulently or dishonestly, obtains the digital health information of another person, which he is not entitled to obtain under the Act from a person or entity storing such information shall be punished with imprisonment for a term which shall extend up to one year or fine, which shall be not less than one lakh rupees; or both.

**40. Data theft**

Whoever intentionally and without authorization acquires or accesses any digital health data shall be punished with imprisonment for a term, which shall extend from three years up to five years or fine, which shall be not less than five lakh rupees; or both.

**41. Cognizance of offences by court**

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made thereunder, save on complaint made by the Central Government, State Government, the National Digital Health Authority of India, State Digital Health Authority, or a person affected.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under sections 36, 39 and 40 of this Act.

**42. Offences by companies**

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time when the contravention was committed, was in charge of and was responsible to the company, for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the contravention, and shall be liable to be proceeded against and punished accordingly.

**Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the commission of such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the

consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

**Explanation 1.**— For the purpose of this Section –

- (a) **“company”** means any body corporate and includes a clinical establishment, entity, firm or other association of individuals; and
- (b) **“director”** in relation to
  - (i) a firm, means a partner in the firm;
  - (ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;

**Explanation 2.**— For the removal of doubts it is hereby clarified that a company may be prosecuted notwithstanding that the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

## CHAPTER VI

### CENTRAL AND STATE ADJUDICATING AUTHORITIES

#### 43. Complaints to State Adjudicating Authority

- (1) For any breach of digital health data by a clinical establishment or any entity an aggrieved person or owner may complain to the State Adjudicatory Authority in writing as may be prescribed, and seek reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;
- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Digital Health Authority under section 38 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.

**44. Complaints to the Central Adjudicating Authority**

- (1) For any breach of digital health data by a health information exchange or State Digital Health Authority or the National Digital Health Authority of India, an aggrieved person or owner may complain to the Central Adjudicatory Authority in writing as may be prescribed, and seek reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;
- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (3) or (4) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the National Digital Health Authority of India under section 38 of this act, may prefer an appeal to the Central Adjudicating Authority under this Act within a period of forty-five days from the date on which a copy of the order is received.
- (6) Any person or entity or owner or State Digital Health Authority, aggrieved by the order of the State Adjudicatory Authority may prefer an appeal to the Central Adjudicatory Authority, within 3 months from the date on which a copy of the order is received.

**45. Adjudicating authorities, composition, powers etc.**

- (1) The Central Government shall by Notification, appoint a Central Adjudicating Authority, and the State Governments shall by notification, appoint State Adjudication Authorities respectively, to exercise jurisdiction, powers and authority conferred by or under this Act
- (2) The Adjudicating Authority, whether Central or State, shall consist of a Chairperson and two other members, provided that at least one of such persons shall be from the field of law.
- (3) A person shall, however, not be qualified for appointment as Member of an Adjudicating Authority –
  - (a) In the field of law, unless he:
    - (i) Is qualified for appointment as District Judge; or
    - (ii) Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
  - (b) In the field of medicine, information (health) science or administration, unless he possesses such qualifications as may be prescribed by the Central Government.
- (4) The Central Government and the State Governments shall appoint the Member from the field of law, to be the Chairperson of the Central Adjudicating Authority and State Adjudicatory Authorities respectively.
- (5) Subject to the provisions of this Act,



- (a) The Central Adjudicatory Authority shall sit at New Delhi...
- (b) The State Adjudicating Authorities shall ordinarily sit at the State Capitals;
- (6) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.

Provided that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.

- (7) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed.

Provided that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.

- (8) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government or the State Governments, as the case may be, shall appoint another person in accordance with the provisions of this Act to fill the vacancy, and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.
- (9) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government or the State Government, as the case may be, resign his office:

Provided that, the Chairperson or any other Member shall, unless he is permitted by the Central or State Government to relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (10) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government or the State Government, as the case may be, after giving necessary opportunity of being heard.
- (11) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in accordance with the provisions of this act to fill such vacancy, enters upon his office.
- (12) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (13) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the

principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

**46. Staff of the adjudicating authority**

- (1) The Central Government shall provide the Central Adjudicating Authority, and the State Governments shall provide the State Adjudicating Authorities, with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees of the Adjudicating Authority shall be such as may be prescribed.

**47. Power regarding summons, production of documents and evidence**

- (1) The Central Adjudicating Authority and State Adjudicatory Authorities shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely
  - (a) Discovery and inspection;
  - (b) Enforcing the attendance of any person, including any officer of a Clinical establishment or a health information exchange and examining him on oath;
  - (c) Compelling the production of records;
  - (d) Receiving evidence on affidavits;
  - (e) Issuing commissions for examination of witnesses and documents; and
  - (f) Any other matter which may be prescribed by the Central Government.
- (2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or make statements, and produce such documents as may be required.
- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

**48. Civil court not to have jurisdiction**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Central Adjudicatory Authority or the State Adjudicatory Authority is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**49. Appeal to High Court**

- (1) Any person aggrieved by any decision or order of the Central Adjudicatory Authority may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Adjudicatory Authority to him on any question of law or fact arising out of such order.
- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

<b>CHAPTER VII</b> <b>MISCELLANEOUS PROVISIONS</b>
---

**50. Act to supersede any other law**

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health data' hereunder.

**51. Power of the Central Government to make rules**

- (1) The Central Government may, by notification in the Official Gazette, make rules for the purposes of carrying out the provisions of this Act.
- (2) Every Rule made by the Central government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament.

**52. Power of the State Government to make Rules –**

- (1) Subject to the other provisions of this Act, the State Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act;
- (2) Every Rule made by the State government under this Act shall as soon as may be after its made, be placed in each House of the State Legislature, where there are two houses.

**53. Removal of difficulty by the government**

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of

consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.

- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

\*\*\*

**Schedule I****Personally Identifiable Information**

- (iv) Name
- (v) Address
- (vi) Date of Birth
- (vii) Telephone Number
- (viii) Email Address
- (ix) Password
- (x) Financial information such as bank account or credit card or debit card or other payment instrument details;
- (xi) Physical, physiological and mental health condition;
- (xii) Sexual orientation;
- (xiii) Medical records and history;
- (xiv) Biometric Information;
- (xv) Vehicle number
- (xvi) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL').

New Issue – we should not disallow direct sharing of identifiable data for direct patient care between two hospitals.

**Digital Healthcare Data Privacy, Confidentiality & Security Act****Comments from Health HFM office and response to it (PHA Div. dated 22<sup>nd</sup> November 2017)**

	<b>Agreed</b>
	<b>To be discussed</b>
	<b>Clarifications</b>

<b>S No.</b>	<b>Comments</b>	<b>Response</b>
Sec 1 Short title	Change the name to “Digital Information Security in Healthcare Act (DISHA)”	Agreed. Draft modified accordingly.
Sec. 2. Commencement & application	Why do we have this provision? – different dates may be appointed for different states and for different provisions of this Act.	Only to provide flexibility, if needed, according to different levels of development and infrastructure in different states. This flexibility does not necessarily have to be used.  Standard Language- has been used in FSSAI, IRDA and Clinical Establishment Act
<b>Sec 3 Definitions</b>		
3(1)(b) 'Breach'	• Section 34 doesn't have anything on breach	Agreed. Reference ought to be to Section 35 (first section in Chapter V) Reference changed according to modified draft
	• Why should a definition be in the main part of the act?	As the definition relates to a substantive provision – which leads to a claim for compensation, it has been defined in the main text with a reference in the definitions.
3(1)(d) 'de-identification'	Is de-identification different from anonymization?	Yes. Hence, different definitions are required.
3(1)(f) Entity	Why are we defining it when general definition exists	<ul style="list-style-type: none"> <li>Defining the term entity ensures the specificity that is sought to be achieved in terms of the coverage of the proposed law.</li> <li>In terms of a general definition, the term “person” is mostly used, but will exclude certain forms of entities, which are not considered to have separate personhood, such as partnerships and trusts etc. Thus, a specific definition would be required.</li> </ul>

3(1)(m) 'relative'	Why are we linking definition of 'relative' to HIV/AIDS Act?	Agreed. The definition can be reproduced here. Draft modified accordingly.
3(1)(o) 'sensitive health-related information'	HIV and STI are circled in the definition.	Agreed. If it is suggested to use full form. Draft modified accordingly.
3(1)(p) 'serious breach'	Why is 'serious breach' not fully defined in the definitions chapter itself?	As the definition relates to a substantive provision – which leads to a claim for compensation, it has been defined in the main text with a reference in the definitions.
<b>CHAPTER 2</b>		
Sec 4 – NDHAI	• Rename it to NeHA	Agreed. However, the name of the State Authority would also change to SeHA. Draft modified accordingly.
	• Why – 'unless the Central Govt. specifies a separate date in the same notification'	It is a standard clause.
Sec 5 – composition	'One' instead of '1'	Agreed. Draft modified accordingly.
	give specific Ministry's name instead of subject area	Agreed. Draft modified accordingly.
	5(2)(b) proviso – "demonstrable qualities of leadership, institution building and commitment". There should be proof of this.	This will be ascertained from the CVs or background of the candidates and there is no need to put in specific requirements of proof in the statute
	5(3) - There should be a separate section on executive cell	Agreed. Draft modified accordingly.
Sec 6 – SDHA	Why – 'unless the Central Govt. specifies a separate date in the same notification'	It is a standard clause.
Sec 7 – SDHA composition	7(1)(b) Secretary ' <u>In-charge of State</u> ' (INSERT) Health Dept. or equivalent...	Agreed. Draft modified accordingly.
	'One' instead of '1'	Agreed. Draft modified accordingly.
	give specific Ministry's name instead of subject area	Agreed. Draft modified accordingly.
	7(3) - There should be a separate section on executive cell	Agreed. Draft modified accordingly.

Sec 8 - Term of office of Chairperson and other members	Remove – ‘as the central govt. may notify in this behalf’	To be discussed
	Term of other members?	Sec 8 covers term of office of Chairperson as well as other members.
	More clarity needed on “another term or such other terms”	It means that the chairperson or members could be re-appointed for another term or more than one other term. However ‘such other terms’ deleted. Draft modified accordingly.
Sec 9 – salary and allowances	Better to give equivalent status to members of both National and State Authorities. It is suggested that the Central government should prescribe salary etc. of members of both the NDHAI and SDHAI.	The salary etc. of Chairperson and full time members of NDHAI to be fixed by Central Government and that of SDHAI to be fixed by State Government.  <b>To be discussed</b>
Sec 11 – temporary association of persons	Norms related to temporary association of persons should be left to regulations and not rules, as rules are more time taking and can be too prescriptive.	To be discussed. However generally these provisions are covered under Rules.
Sec 13. Meetings	Why are we saying ‘provided by regulations’	Agreed that we can just say prescribed and it can be covered by rules which would also cover the above subject matter.
Sec 14. Disqualifications	(i) Has been convicted and sentenced to imprisonment for an offence which in the opinion of the C. Govt. involves moral turpitude. It is vague. Link it to IPC.	It is not vague. It clearly says ‘convicted and sentenced for an offence’ This makes it broader than conviction for an offence only under IPC.
Sec 17 HIEs	<ul style="list-style-type: none"> <li>No clear definition.</li> <li>Circular reference to HIE in Sec 2.</li> </ul>	Agreed. HIEs can be defined. Draft modified accordingly.
Sec 18 – management of HIEs	18(3) conditions with respect to periodical reports, annual reports and direct inquiries may be such as may be prescribed. This should be left to Authority and shouldn’t be prescribed by Rules.	These were earlier part of the Act but was thought to be moved to the Rules.  These should be covered in Rules for greater accountability of HIEs.
Sec 19 – CHIE functions	19(1) - The qualifications and experience of CHIE should not be prescribed by NDHAI but by the rules under the Act.	It could be moved to Rules instead. Draft modified accordingly.
	19(2) - The section reference no. needs to be corrected	Agreed. Will be corrected.



	19(2)(b) – HIE will access and process the digital health care data transmitted by clinical establishments – “Why only from CE?”	It was not mandated that the other entities will transfer data to HIEs from their surveys etc. Hence, the exclusion. To be discussed
<b>CHAPTER 3</b>		
Sec 20 - Powers and functions of NDHAI	20(1)(a)(ii) – the sentence is confusing and needs to be redrafted	Agreed. Draft modified accordingly.
	20(1)(a)(iv) – Can the NDHAI make protocols/standards pertaining to digital data which would be applicable to itself as well?	Yes, it can. Or, we could move it to the Rules? To be discussed.
	20(1)(d) – notify and mandate the HIE. ‘notify and mandate’ has been circled.	Not clear what exactly the comment is. But it can be discussed whether ‘notify and mandate’ are the correct words to use.
	20(1)(e) – whether we should use the term ‘abroad’?	We could use ‘other countries’ instead?? Draft modified accordingly.
Sec 21 – NDHAI’s power of oversight etc..	<p>proviso to Sec 21 (1) – “provided that NDHAI while accessing such records or accessing either the physical or virtual premises of HIE shall bear in mind that no or least possible hindrance is caused to the normal working of the HIE.</p> <p>Comment – may have to be stopped in event of a virus attack</p>	It is understood that such precautions will be undertaken by NDHAI
Sec 22 – powers and functions of SDHA	‘conduct investigations’ and ‘notify and mandate’ have been circled.	Not clear what the comment exactly is. Probably questions the use of those words?
	22(2) – after prescribed mention by who	Agreed. Draft modified accordingly.
Sec 25 – power to give directions	<p>Every CE shall be bound by such directions in writing as the State Authority may give to it.</p> <p>Comment – NDHAI cannot give directions to CEs?</p>	The NDHAI will supervise the HIE and the SDHA will supervise the CEs. That’s why this division in power to give directions. However, this can be discussed.
<b>CHAPTER 4</b>		

Sec 26 – rights of owner of digital data	Sec 26(8)(b) – mention prescribed by whom?	Agreed. Draft modified accordingly.
	Sec 26(8)(g) – right to seek compensation by damages caused by breach of health data.  Comment – How will the damage be calculated?	This is mostly a judicial exercise. The court decided on the quantum of compensation depending on the type of data breached and the extent of damage caused. We should leave it to the courts to decide on facts and circumstances of each individual case.
Sec 27 (2)	The provision is not clear – ‘digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (C) of sub-sec.1	Section 27(2) is applicable to entities other than clinical establishments, which is Section 27(1). So entities under Section 27(2), like say TIs or any charitable trust providing medical services can generate, collect and store digital health data only for the purposes mentioned in Section 27(1)(a) to (c), i.e., for individualised medical services, and to provide better effective medical care. Section 27(1)(d) to (h) are meant for broader public health purposes.
Sec 27 (5) Explanation about insurance companies not insisting on accessing	Specified by the govt., mention which government.	Agreed
	Role of IRDA?	Not clear what the query is  Role of IRDA: IRDA has been set up to regulate the insurance sector, which the current law does not interfere with. The provisions of the present law only regulate digital health data and proviso under consideration regulates digital health data and its use by insurance companies. Thus, this law does not infringe on the jurisdiction of IRDA.
	Role of courts?	Role of courts: Violation of this provision will amount to a breach under this Act, for which the fora provided may be approached

<p>Sec. 28 – collection of health data</p>	<p>28(2) A CE may, by consent from the owner, recorded in the form and manner as may be prescribed under the Act, lawfully collect the required health data as per the regulations prescribed by the NDHAI ...</p> <p>Comment – why are there two prescriptions?</p>	<p>first prescription related to the format in which consent will be sought.</p> <p>Second prescription is about the protocols etc related to collection of digital data. But this can be discussed too.</p>
	<p>28(2)(c) and (d) – states that the informed consent of the owner should be taken after informing him/her of the identity of recipients to whom data may be sent or disclosed and identity of recipients who may have access to such digital data on a need to know basis.</p> <p>Comment – what about transmissions to be done in the future?</p>	<p>All transmissions, whether immediate or future are covered.</p> <p>With regard transfers in the future, they may be done only with the consent of the person in terms of Section 31(3)</p>
	<p>Sec 28(6) – how does one decide what is ‘in the best interest of the minor’?</p>	<p>It is to be decided by a health care provider, on good faith, exercising her/his own judgement. If this is challenged then it gets decided by the court.</p> <p>Although there is no standard definition of “best interests of the child,” the term generally refers to the deliberation that courts undertake when deciding what type of services, actions, and orders will best serve a child. “Best interests” determinations are generally made by considering a number of factors related to the child’s circumstances and the parent or caregiver’s circumstances and capacity to parent, with the child’s ultimate safety and well-being the paramount concern.</p>
<p>Sec 31 – Transmission of data</p>	<p>Proviso to 31(2) – don’t use the word notification. Use Rules/ regulation/standards</p> <p>Who will prescribe the form and manner in which the HIE has to maintain register?</p>	<p>Add ‘by the Central Government after’ ‘prescribe’</p>

# **Digital Information Security in Healthcare, Act**

***[Draft for Public Consultation]***

**November, 2017**

**Ministry of Health & Family Welfare,  
Government of India**

**INDEX**

<b>SL. NO.</b>	<b>PARTICULARS</b>	<b>PAGE NO.</b>
1	CHAPTER I – PRELIMINARY	2
2	CHAPTER II - NATIONAL ELECTRONIC HEALTH AUTHORITY	6
	STATE ELECTRONIC HEALTH AUTHORITIES	
	HEALTH INFORMATION EXCHANGES	
3	CHAPTER III – POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES	13
4	CHAPTER IV - DATA OWNERSHIP, SECURITY AND STANDARDIZATION	
5	CHAPTER V- DIGITAL HEALTH DATA BREACH AND CONSEQUENCES	24
6	CHAPTER VI- ADJUDICATING AUTHORITY	27
7	CHAPTER VII- MISCELLANEOUS PROVISIONS	31

## Digital Information Security in Healthcare Act (INSERT YEAR)

*An Act to provide for establishment of National and State eHealth Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data and such other matters related and incidental thereto.*

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

### CHAPTER I PRELIMINARY

#### 1. SHORT TITLE, EXTENT

- (1) This Act may be called as Digital Information Security in Healthcare Act (DISHA) (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

#### 2. COMMENCEMENT AND APPLICATION

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.

#### 3. DEFINITIONS

- (1) In this Act, unless the context otherwise requires,
  - (a) **'Anonymization'** means the process of permanently deleting all personally identifiable information from an individual's digital health data.
  - (b) **'Breach'** shall have the same meaning as assigned to it in Section 37 of this Act.
  - (c) **'Consent'** means expressed informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.

Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.

- (d) **'De-identification'** means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that

eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.

- (e) **‘Digital Health Data’** means an electronic record of health-related information about an individual and shall include the following:
  - (i) Information concerning the physical or mental health of the individual;
  - (ii) Information concerning any health service provided to the individual;
  - (iii) Information concerning the donation by the individual of any body part or any bodily substance;
  - (iv) Information derived from the testing or examination of a body part or bodily substance of the individual;
  - (v) Information that is collected in the course of providing health services to the individual; or
  - (vi) Information relating to details of the clinical establishment accessed by the individual.
- (f) **‘Entity’** includes any of the following, not being a clinical establishment:
  - (i) An individual;
  - (ii) A company;
  - (iii) A department of the Central or State Government;
  - (iv) A firm;
  - (v) An association of persons or a body of individuals, whether incorporated or not, in India or outside India; or
  - (vi) Any corporation established by or under any Central, State or Provincial Act or a Government company as defined in section 2(45) of the Companies Act, 2013;
  - (vii) Any body corporate incorporated by or under the laws of a country outside India;
  - (viii) A co-operative society registered under any law relating to cooperative societies;
  - (ix) A local authority;
  - (x) Every artificial juridical person, not falling within any of the preceding sub-clauses;
- (g) **‘Guardian’** means a guardian recognised under any law for the time being in force.
- (h) **‘Health Information Exchange’** means a health information exchange as established under this Act.

- (i) **‘Clinical Establishment’** means (i) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicines established and administered or maintained by any person or body of persons, whether incorporated or not; or (ii) a place established as an independent entity or part of an establishment referred to in sub-clause (i), in connection with the diagnosis where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not, and shall include a clinical establishment owner, controlled or managed by
- a. the Government or a department of the Government;
  - b. a trust, whether public or private;
  - c. a corporation (including a society) registered under a Central, Provincial or State Act, whether or not owned by the Government;
  - d. a local authority;
  - e. a single doctor,
- but does that include the clinical establishments owned, controlled or managed by the Armed Forces.  
Explanation: For the purpose of this clause, “Armed Forces” means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)
- (j) **‘Owner’** means an individual whose digital health data is generated and processed under this Act.
- (k) **‘Personally Identifiable Information’** means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I.
- (l) **‘Prescribed’** shall mean rules prescribed by the Central Government or the State Governments as the case may be.
- (m) **‘Relative’** with reference to the owner, means—
- (i) spouse of the owner;
  - (ii) parents of the owner;
  - (iii) brother or sister of the owner;



- (iv) brother or sister of the spouse of the owner;
  - (v) brother or sister of either of the parents of the owner;
  - (vi) in the absence of any of the relatives mentioned at sub-clauses (i) to (v), any lineal ascendant or descendant of the owner;
  - (vii) in the absence of any of the relatives mentioned at sub-clauses (i) to (vi), any lineal ascendant or descendant of the spouse of the owner;
- (n) **‘Data Security’** refers directly to protection of digital health data, and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.
- (o) **‘Sensitive health-related information’** means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, Human Immunodeficiency Virus status, Sexually Transmitted Infections treatment, and abortion.
- (p) **‘serious breach’** shall have the same meaning as assigned to it in Section 38 of this Act.
- (q) **‘Specified’** shall mean as specified by National eHealth Authority of India or State eHealth Authority, as the case may be.
- (r) **“need to know basis”** means the access to digital health data by a specific person for a specific and lawful purpose that is necessary for that purpose or to carry out that function.

## CHAPTER II

### NATIONAL ELECTRONIC HEALTH AUTHORITY OF INDIA, STATE ELECTRONIC HEALTH AUTHORITIES AND HEALTH INFORMATION EXCHANGES

#### 4. National Electronic Health Authority of India (NeHA)

- (1) The Central Government shall establish for the purposes of this Act, a National Electronic Health Authority of India, by Notification in the

Official Gazette, which may be referred to as NeHA in its abbreviated form.

- (2) The National Electronic Health Authority of India, shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government, specifies a separate date in the same Notification.

#### **5. Composition of National Electronic Health Authority of India**

- (1) National Electronic Health Authority of India shall consist of the following members, to be appointed by the Central Government by Notification, namely:
  - (a) A full time Chairperson;
  - (b) A member -secretary; equivalent to the rank of Joint Secretary to the Government of India
  - (c) Four full-time members to be appointed by the Central Government:
    - (i) One from health informatics;
    - (ii) One from public health;
    - (iii) One from law; and
    - (iv) One from public policy
  - (d) Four ex-officio members, not less than the rank of Joint Secretary to the Government of India to be appointed by the Central Government:
    - (i) One from Ministry of Electronics and Information Technology;
    - (ii) One from Ministry of Panchayati Raj/ Ministry of Women & Child Development;
    - (iii) One from Directorate General of Health Services; and
    - (iv) One from Ministry of Law and Justice
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
  - (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Fifteen years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.

Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.

- (3) The National Authority shall be a body corporate with the name specified by the Central Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and

dispose of property and to contract, and may, by the said name, sue or be sued.

#### **6. National Executive Committee**

- (1) The Central Government shall, immediately after the notification under sub-section (1) of Section 4, constitute a National Executive Committee to assist the National Authority in the performance of its functions under this Act.
- (2) The National Executive Committee shall consist of the following members, namely:-
  - (a) Additional Secretary/Joint Secretary, ehealth as Chairperson;
  - (b) Deputy Commissioner/Assistant Commissioners as members;
  - (c) Director/Deputy Secretary as member; and
  - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the National Executive Committee may invite any other officer of the Central Government or a State Government for taking part in any meeting of the National Executive Committee and shall exercise such powers and perform such functions as may be prescribed by the Central Government in consultation with the National Authority.
- (4) The procedure to be followed by the National Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the Central Government.

#### **7. State Electronic Health Authorities**

- (1) Every State Government shall, as soon as may be after the issue of the notification under sub-section (1) of section 4, by notification in the Official Gazette, establish a State Electronic Health Authority, which may be referred to as SeHA in its abbreviated form.
- (2) The State Electronic Health Authority shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the State Government, specifies a separate date in the same Notification.

#### **8. Composition of State Electronic Health Authorities**

- (1) State Electronic Health Authority shall consist of the following members, to be appointed by the State Government by Notification, namely:
  - (a) A full time Chairperson;
  - (b) Secretary in-charge of State Health Department or equivalent as member-secretary;
  - (c) Three full-time members to be appointed by the State Government:
    - (i) One from health informatics;
    - (ii) One from public health; and
    - (iii) One from law

- (d) Three ex-officio members to be appointed by the State Government:
  - (i) Director, State Health Services;
  - (ii) One from State Information Technology department; and
  - (iii) One from State Law department
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
  - (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Twelve years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.

Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.
- (3) The State Authority shall be a body corporate with the name specified by the State Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and dispose of property and to contract, and may, by the said name, sue or be sued.

## **9. State Executive Committee**

- (1) The State Government shall, immediately after issue of notification under sub-section (1) of section (7), constitute State Executive Committee to assist the State Authority in the performance of its functions, under this Act.
- (2) The State Executive Committee shall consist of the following members, namely:—
  - (a) The Secretary Health, as the Chairperson;
  - (b) Director, Health Services as member;
  - (c) Deputy Secretary ehealth as member; and
  - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the State Executive Committee shall exercise such powers and perform such functions as may be prescribed by the State Government and such other powers and functions as may be delegated to him by the State Authority.
- (4) The procedure to be followed by the State Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the State Government.

## **10. Term of Office of Chairperson & other members of National and State Authorities**

- (1) The Chairperson and members of the National Authority, shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (2) The chairperson and members of the State Authority, shall hold office for a term of three years, as the State Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (3) The Chairperson and other Members, appointed as per sub-section (1) of section 5 and sub-section (1) of section 8, are eligible for reappointment for another term; provided such reappointed Chairperson or Member does not exceed sixty-five years of age.

#### **11. Salary, allowance, benefits and service conditions etc.,**

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the National Authority, shall be such as may be prescribed by the Central Government.
- (2) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the State Authorities, shall be such as may be prescribed by the State Governments.
- (3) Notwithstanding anything stated in sub-section (1) and (2) above, the salary, allowances and other conditions of service of the Chairperson or of a member shall not be varied to his disadvantage after his appointment.

#### **12. Reconstitution of the National and State Authorities**

- (1) Any vacancy caused to the office of the Chairperson or any other member of the National & State Authority shall be filled up by the Central Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (2) Any vacancy caused to the office of the Chairperson or any other member of the State Authority shall be filled up by the State Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (3) In the event of vacancy in the office of the Chairperson of the National or State Authority, the senior most person, from amongst the full time members, shall act as the Chairperson, till the vacancy is filled.
- (4) No act or proceeding of the National or State Authority shall be invalid merely by reason of-
  - (a) Any vacancy in, or any defect in the constitution of the Authority; or
  - (b) Any defect in the appointment of a person acting as a member of the Authority; or

- (c) Any irregularity in the procedure of the Authority not affecting the merits of the case.

### **13. Temporary association of persons with National or State Authorities for particular purposes –**

- (1) The National Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (2) A State Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (3) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall have a right to take part in the discussions of the Authority relevant to that purpose, but shall not have a right to vote at a meeting of the Authority, and shall not be a member for any other purpose.
- (4) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall be paid such fees and allowances, for attending its meetings and for attending to any other work of the Authority, as may be prescribed.

### **14. Officers and Other Employees of the National and State Authorities**

- (1) The National Authority, in consultation with Central Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (2) The State Authority, in consultation with the State Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (3) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the National or State Authority appointed under sub-section (1) and (2) shall be such as may be prescribed.

### **15. Meetings**

- (1) The National Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (2) The State Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (3) The chairperson of the National or State Authority, if unable to attend a meeting, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

**16. Disqualifications**

- (1) A person shall be disqualified for appointment as Chairperson or member of the National Electronic Health Authority or a State Electronic Health Authority, if he/she –
  - (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (ii) Is an undercharged insolvent; or
  - (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
  - (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
  - (v) Has such other disqualification as may be prescribed by the Central Government.

**17. Resignation, removal of chairperson or member of the National or State Authorities**

- (1) The Chairperson or full time member of the National Authority appointed under sub-section (1) of section 5 and the Chairperson or full time member of a State Authority appointed under sub-section (1) of section 8:
  - (a) May relinquish his/her office by submitting the resignation in writing to the Central Government or the State Government as the case may be; or
  - (b) May be removed from his/her office in accordance with the provisions of section 18.

**18. Removal in certain circumstances**

- (1) The Central Government or the State Government, may remove from office the Chairperson or any full-time member of the National or State Authority, who –
  - (a) Has been adjudged as an insolvent; or
  - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (c) Has become physically or mentally incapable of discharging his or her functions; or
  - (d) Has acquired such financial or other interest as is likely to affect prejudicially his or her functions as the Chairman or member; or
  - (e) Has so abused his/her position as to render his or her continuance in office prejudicial to the public interest.
- (2) No such member or Chairperson shall be removed from his/her office under clause (d) or clause (e) of sub-section (1) above, unless he/she has been given a reasonable opportunity of being heard in the matter.

**19. Health Information Exchanges**

- (1) The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act
- (2) No entity shall function as a Health Information Exchange unless established as such by the central Government

**20. Management of Health Information Exchange**

- (1) All Health Information Exchanges shall conduct and carry out their affairs strictly as per the norms, standards or protocols specified by the National Electronic Health Authority, from time to time, or as per the Rules prescribed by the Central Government.
- (2) Without prejudice to any other stipulations of this Act, a Health Information Exchange established under section 19 shall only employ such skilled personnel for management of its affairs as may be specified by the National Electronic Health Authority.
- (3) Conditions with respect to periodical reports, annual reports and direct inquiries may be such as may be prescribed by the Central Government.

**21. The Chief Health Information Executive and his functions**

- (1) The Health Information Exchange shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the Central Government as rules under this Act;
- (2) The Chief Health Information Executive as appointed under sub-section (1) above, shall be the Chief Executive Officer and also the data controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs, and in particular:
  - (a) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
  - (b) Access, and process the digital health care data transmitted by the Clinical Establishments to further transmit the digital health care data, whenever required, in accordance with norms prescribed by the National Electronic Health Authority of India.
  - (c) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
  - (d) Notify the data breach to the owner and such other concerned.
  - (e) Store the digital health care data in prescribed mode in all situations.



CHAPTER III  
POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES

**22. Powers and functions of National Electronic Health Authority of India**

- (1) The National Electronic Health Authority of India in order to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Formulate standards, operational guidelines and protocols for the generation, collection, storage and transmission of the digital health data for the purposes of this Act, applicable to:
    - (i) Clinical establishments generating and collecting digital health data for their own use or for further transmission to the health information exchanges;
    - (ii) Health information exchanges storing and transmitting digital health data to clinical establishments, or to other health information exchanges, or to State Electronic Health Authority, or the National Electronic Health Authority;
    - (iii) Any other entity having custody of any digital health data;
    - (iv) State Electronic health Authority and the National Electronic Health Authority;
  - (b) To ensure data protection and prevent breach or theft of digital health data, establish data security measures for all stages of generation, collection, storage and transmission of digital health data, which shall at the minimum include access controls, encrypting and audit trails;
  - (c) Conduct periodical investigations to ensure compliance with the provisions of this Act and any rules, regulations, standards or protocols hereunder by health information exchanges;
  - (d) Notify and mandate the health information exchanges, in case of failure to comply with the provisions of this Act;
  - (e) To lay down protocol for transmission of digital health data to and receiving it from other countries;
  - (f) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
  - (g) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed

**23. National Authority's power of oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the National Electronic Health Authority or its representative, shall have the right to inspect all such records; or access the premises, including virtual premises of the health information exchange or exchanges at any time.

**Provided** that National Electronic Health Authority, while accessing such records or accessing either the physical or virtual premises of health information exchanges, shall bear in mind that no or least possible hindrance is caused to the normal working of the health information exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Electronic Health Authority to generally discharge its functions under this Act, shall direct a health information exchange or class of health information exchanges, or all health information exchanges as the case may be, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the National Electronic Health Authority, shall be binding upon the health information exchange or health information exchanges.

**24. Powers and Functions of State Electronic Health Authorities**

- (1) The State Electronic Health Authority to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Ensure that the clinical establishments and other entities in the state collect, store, transmit and use digital health data as per the provisions of this Act and the standards, protocols and operational guidelines issued by the National Electronic Health Authority, from time to time;
  - (b) Conduct investigations to ensure compliance with the provisions of this Act;
  - (c) Notify and mandate the clinical establishments and other entities, in case of failure to comply with the provisions of this Act;
  - (d) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (c) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed by the Central Government.

**25. State Authority's power of Oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the State Electronic Health Authority, or its representative, shall have the right to inspect all such records; or access the premises including virtual premises, of a Clinical establishment or other entities at any time.

**Provided** that State Electronic Health Authority while accessing such records or accessing the physical premises of Clinical establishments, shall bear in mind that no or least possible hindrance is caused to the normal working of the clinical establishment

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the State Electronic Health Authority to generally discharge its functions under this Act, it shall direct a clinical establishment or a class of clinical establishments, or all clinical establishments as the case may be, or entities, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the State Digital Health Authority are binding upon the clinical establishment or clinical establishments and entities as the case may be.

**26. Power of Civil Court –** Notwithstanding anything contained in any other law for the time being in force, the National Authority while exercising the powers under section 23 and the State Authorities while exercising the powers under section 25, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-

- (a) summoning and enforcing the attendance of witnesses and examining them on oath;
- (b) discovery and production of any document;
- (c) receiving evidence on affidavit;
- (d) requisitioning any public record or copy thereof from any court or office;
- (e) issuing commissions for examination of witnesses or documents;
- (f) any other matter which may be prescribed

**27. Power to give directions –**

- (1) In the performance of its functions under this Act, -
  - (a) The National Authority shall be bound by such directions in writing as the Central Government may give to it;
  - (b) Every State Authority shall be bound by such direction in writing as the National Authority or the State Government may give to it;

*Provided that* where a direction given by the State Government is inconsistent with the direction given by the National Authority, the matter shall be referred to the Central Government for its decision, which shall be final.

- (c) Every Health Information Exchange shall be bound by such directions in writing as the National Authority may give to it;
- (d) Every Clinical Establishment shall be bound by such directions in writing as the State Authority may give to it.

#### CHAPTER IV

##### DATA OWNERSHIP, SECURITY AND STANDARDIZATION

#### **28. The rights of the owner of digital health data**

- (1) An owner shall have the right to privacy, confidentiality, and security of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.
- (2) An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 29 of this Act.
- (3) An owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data.
- (4) An owner shall have the right to refuse consent to the access or disclosure of his or her digital health data, and if refused it shall not be disclosed, subject to the exceptions provided in Section 33 of the Act.
- (5) An owner of the digital health data shall have the right that the digital health data collected must be specific, relevant and not excessive in relation to the purpose or purposes for which it is sought;
- (6) An owner of the digital health data shall have the right to know the clinical establishments or entities which may have or has access to the digital health data, and the recipients to whom the data is transmitted or disclosed;
- (7) The owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any Clinical Establishment/Entity;
- (8) The owner of the digital health data shall have, subject to sub-section (1) to (3) above:
  - (a) The right to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data, in the prescribed form as may be notified by the National Electronic Health Authority;
  - (b) The right to require their explicit prior permission for each instance of transmission or use of their digital health data in

- an identifiable form, through such means as may be prescribed by the Central Government;
- (c) The right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 34 of the Act;
- (d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;
- (e) The right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner;
- (f) The right not to be refused health service, if they refuse to consent to generation, collection, storage, transmission and disclosure of their health data;
- (g) The right to seek compensation for damages caused by a breach of digital health data.

**29. Purposes of collection, storage, transmission and use of the digital health data**

- (1) Digital health data may be generated, collected, stored, and transmitted by a clinical establishment and; collected, stored and transmitted by health information exchange, for the following purposes:
  - (a) To advance the delivery of patient centered medical care;
  - (b) To provide appropriate information to help guide medical decisions at the time and place of treatment;
  - (c) To improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;
  - (d) To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;
  - (e) To facilitate health and clinical research and health care quality;
  - (f) To promote early detection, prevention, and management of chronic diseases;
  - (g) To carry out public health research, review and analysis, and policy formulation;
  - (h) To undertake academic research and other related purposes

Provided that personally identifiable information may only be used for the purposes of direct care of the owner of the data, as specified in clauses (a) to (c) of sub-section (1), subject to provisions of section 28, to the extent considered necessary, and in the best interest of the owner

Provided further that for public health related purposes mentioned in clauses (d) to (h) of sub-section (1), only de-identified or anonymized data shall be used, in the manner as may be prescribed under this Act.

- (2) Digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (c) of Sub-Section (1).
- (3) Digital health data shall not be used for any other purpose, except in accordance with the provisions of this Act.

Provided that the digital health data shall be used only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to use the information.

- (4) There shall be no access to, or disclosure of personally identifiable information, except in accordance with the provisions of this Act.

Provided that the digital health data shall be accessed or disclosed only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to access or disclose the information.

- (5) Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government.

Explanation: Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim.

Provided that for the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates

### **30. Collection of health data**

- (1) No health data shall be collected, for the purposes of conversion to digital health data, by any clinical establishment, or any other entity in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may, by consent from the owner, recorded in the form and manner as may be prescribed under this Act, lawfully collect the required health data, after informing the owner of the following:

- (a) The rights of the owner as laid down in this Act, including the right to refusal to give consent to the generation and collection of such data;
- (b) The purpose of collection of such health data;
- (c) The identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format;
- (d) The identity of the recipients who may have access to such digital health data on a need to know basis
- (3) A clinical establishment or any other entity, shall furnish a copy of the consent form to the owner.
- (4) Any other entity that collects any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data.
- (5) Without prejudice to the above sub-section (2), when an individual is incapacitated or incompetent to provide consent, either due to physical or mental incapacity, the clinical establishment may collect health data by obtaining proxy consent from a nominated representative, relative, care giver or such other person, as may be prescribed under this Act, and who has the legal capacity to consent.

Provided that where the individual has regained his or her capacity to give or refuse consent for the collection of his or her health data by the clinical establishment, he or she shall have the option to seek withdrawal of proxy consent and obtaining his or her own consent for collection of such health data, in such form and manner as may be prescribed by the National Electronic Health Authority of India.

- (6) Where a person is a minor and it is in the best interest of the minor, proxy consent can be obtained by the minor's legal guardian, or representative.

Provided that upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.

### **31. Ownership of digital health data**

- (1) The digital health data generated, collected, stored or transmitted shall be owned by the individual whose health data has been digitised;
- (2) A clinical establishment or Health Information Exchange shall hold such digital health care data referred to in sub-section (1) above in trust for the owner;
- (3) Any other entity who is in custody of any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data;
- (4) Notwithstanding anything stated in the above sub-sections (1) to (3), the medium of storage and transmission of digital health data shall be

owned by the clinical establishment or health information exchange, as the case may be.

### 32. Storing of digital health data

- (1) No digital health data shall be stored by any clinical establishment or entity or health information exchange in any manner, except in accordance with the provisions of this Act.
- (2) The clinical establishment or health information exchange, as the case may be, shall hold all digital health data, on behalf of National Electronic Health Authority; and such data be used for such purposes as stated in Section 29, without compromising the privacy or confidentiality of the owner, and security of such data.
- (3) The digital health data vested with the National Electronic Health Authority as per sub-section 2 above, shall be stored and may be transmitted or used in such form and manner as may be prescribed by the National Electronic Health Authority.

### 33. Transmission of data

- (1) No digital health data shall be transmitted by a clinical establishment or health information exchange, or any other entity, as the case may be, in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the clinical establishment.

**Provided** that for such secure, encrypted and instantaneous transmission of digital health data as referred in sub-section (2), the National Electronic Health Authority of India shall prescribe appropriate standards for physical, administrative and technical measures, keeping in mind the privacy and confidentiality of the owner, by notification

- (3) The digital health data shall be transmitted by a clinical establishment or entity or health information exchange only upon the consent of the owner, after being informed of the rights of the owner under Section 28, and the specific purposes of collection of such data under Section 29.
- (4) A health information exchange shall maintain a register in such form and manner as may be prescribed by the Central Government, containing all details of the transmission of the digital health data between a clinical establishment and health information exchange, and between health information exchanges *inter se*.

### 34. Access to digital health data

- (1) No digital health data collected, stored or transmitted by a clinical establishment or health information exchange, as the case may be,



shall be accessed by any person, except in accordance with the provisions of this Act.

- (2) The digital health data collected or stored or transmitted by a clinical establishment or health information exchange, as the case may be, may be accessed by the clinical establishment, on a need to know basis, in such form and manner as may be prescribed under this Act.
- (3) The government departments through their respective Secretaries, may submit request for digital health data in de-identified/anonymized form, to the National Electronic Health Authority, in the form and manner specified by the Authority, subject to provisions of clauses (d) to (h) of sub-section (1) of section 29 of this act.

Provided that the National Electronic Health Authority of India may prescribe any other class of persons who may access digital health data, which is anonymized, for the purposes stated in clause (d) to (h) of sub-section (1) of section 29 of the Act.

- (4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for administration of justice, such access may be granted to an investigating authority only with the order of the competent court;
- (5) The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India.
- (6) In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified;
- (7) In case of an emergency, the relatives of the owner may have access to such data for the purpose of correct treatment of the owner, subject to such conditions as may be prescribed under this Act.
- (8) In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Electronic Health Authority of India.

Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.

Provided further that in case of death of the owner, the National Electronic Health Authority, shall use the digital health data only in anonymized form.

- (9) All clinical establishments and health information exchanges shall maintain a register in a digital form to record the purposes and usage of digital health data accessed within the meaning of this Section, in such form and manner, as may be specified by the National Electronic Health Authority.

### **35. Duty to maintain privacy and confidentiality of digital health data**

- (1) A clinical establishment, health information exchange, State Electronic Health Authority and the National Electronic Health Authority, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner;
- (2) Any other entity, which has generated and collected digital health data, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner.
- (3) The privacy, confidentiality and security of digital health data shall be ensured by taking all necessary physical, administrative and technical measures, that may be prescribed or specified, to ensure that the digital health data, collected, stored and transmitted by them, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.
- (4) Without prejudice to the above provisions, a clinical establishment or health information exchange shall ensure through regular training and oversight that their personnel comply with the security protocols and procedures as may be prescribed or specified under this act.
- (5) A clinical establishment, or a health information exchange, shall provide notice immediately, and in all circumstances not later than three working days to the owner, in such manner as may be prescribed under this Act, in case of any breach or serious breach of such digital health data.

### **36. Procedure for rectification of digital health data**

- (1) An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed under this Act.
- (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.

## CHAPTER V OFFENCES AND PENALTIES

### **37. Breach of digital health data**

- (1) Digital health data is said to be breached, if:
  - (a) any person generates, collects, stores, transmits or discloses digital health information in contravention to the provisions of Chapter II of this Act; or

- (b) Any person does anything in contravention of the exclusive right conferred upon the owner of the digital health data; or
  - (c) Digital health data collected, stored or transmitted by any person is not secured as per the standards prescribed by the Act or any rules thereunder; or
  - (d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data.
- (2) Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place.

### **38. Serious breach of digital health data:**

- (1) A serious digital health data breach shall be said to have taken place, if:
- (a) A person commits a breach of digital health data intentionally, dishonestly, fraudulently or negligently; or
  - (b) Any breach of digital health data occurs, which relates to information which is not anonymised or de-identified; or
  - (c) A breach of digital health data occurs where a person failed to secure the data as per the standards prescribed by the Act or any rules thereunder; or
  - (d) Any person uses the digital health data for commercial purposes or commercial gain; or
  - (e) An entity, clinical establishment or health information exchange commits breach of digital health data repeatedly;

Explanation: The terms “dishonestly” and “fraudulently” shall have the same meaning as assigned to them under the Indian Penal Code, 1860

- (2) Any person who commits a serious breach of health care data shall be punished with imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.

Provided that, any fine imposed as part of sub-section (2) may be provided to the individual whose data is breached, by the Court, as it deems fit as compensation.

### **39. Compensation for serious breach of digital health information**

- (1) A person or an entity committing a serious breach of digital health information shall be liable to pay damages by way of compensation to the owner of the digital health data in relation to which the breach took place.
- (2) Where any compensation has been awarded under sub-section (2) of section 37, it shall be taken into account when determining the claim made by the person affected.

**40. Penalty for failure to furnish information, return or failure to observe rules and directions, etc.,**

- (1) If any person required under this Act or any rules made thereunder, fails to furnish any information or document or books or returns or reports etc., within the time specified, to National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (2) Any person required under this Act or any rules made thereunder fails to comply, within the time specified, with directions issued by the National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (3) Any person which is required under this Act or any rules made thereunder, after having been called upon by the National Electronic Health Authority in writing, or the State Electronic Health Authority, as the case may be, to redress the grievances of owners of digital healthcare data, fails to redress such grievances within the time specified, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees.

**41. Obtaining the digital health information of another person**

Whoever, fraudulently or dishonestly, obtains the digital health information of another person, which he is not entitled to obtain under the Act from a person or entity storing such information shall be punished with imprisonment for a term which shall extend up to one year or fine, which shall be not less than one lakh rupees; or both.

**42. Data theft**

Whoever intentionally and without authorization acquires or accesses any digital health data shall be punished with imprisonment for a term, which shall extend from three years up to five years or fine, which shall be not less than five lakh rupees; or both.

**43. Cognizance of offences by court**

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made thereunder, save on complaint made by the Central Government, State Government, the National Electronic Health Authority of India, State Electronic Health Authority, or a person affected.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under sections 38, 41 and 42 of this Act.

**44. Offences by companies**

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time when the contravention was committed, was in charge of and was responsible to the company, for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the contravention, and shall be liable to be proceeded against and punished accordingly.

**Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the commission of such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

**Explanation 1.**— For the purpose of this Section —

- (a) **“company”** means any body corporate and includes a clinical establishment, entity, firm or other association of individuals; and
- (b) **“director”** in relation to
- (i) a firm, means a partner in the firm;
  - (ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;

**Explanation 2.**— For the removal of doubts it is hereby clarified that a company may be prosecuted notwithstanding that the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

CHAPTER VI
------------

CENTRAL AND STATE ADJUDICATING AUTHORITIES
--

**45. Complaints to State Adjudicating Authority**

- (1) For any breach of digital health data by a clinical establishment or any entity an aggrieved person or owner may complain to the State Adjudicatory Authority in writing as may be prescribed, and seek

reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;

- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Electronic Health Authority under section 40 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.

#### **46. Complaints to the Central Adjudicating Authority**

- (1) For any breach of digital health data by a health information exchange or State Electronic Health Authority or the National Electronic Health Authority of India, an aggrieved person or owner may complain to the Central Adjudicatory Authority in writing as may be prescribed, and seek reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;
- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (3) or (4) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the National Electronic Health Authority under section 40 of this act, may prefer an appeal to the Central Adjudicating Authority under this Act within a period of forty-five days from the date on which a copy of the order is received.
- (6) Any person or entity or owner or State Electronic Health Authority, aggrieved by the order of the State Adjudicatory Authority may prefer an appeal to the Central Adjudicatory Authority, within 3 months from the date on which a copy of the order is received.

#### **47. Adjudicating authorities, composition, powers etc.**

- (1) The Central Government shall by Notification, appoint a Central Adjudicating Authority, and the State Governments shall by notification,

appoint State Adjudication Authorities respectively, to exercise jurisdiction, powers and authority conferred by or under this Act

- (2) The Adjudicating Authority, whether Central or State, shall consist of a Chairperson and two other members, provided that at least one of such persons shall be from the field of law.
- (3) A person shall, however, not be qualified for appointment as Member of an Adjudicating Authority –
  - (a) In the field of law, unless he:
    - (i) Is qualified for appointment as District Judge; or
    - (ii) Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
  - (b) In the field of medicine, information (health) science or administration, unless he possesses such qualifications as may be prescribed by the Central Government.
- (4) The Central Government and the State Governments shall appoint the Member from the field of law, to be the Chairperson of the Central Adjudicating Authority and State Adjudicatory Authorities respectively.
- (5) Subject to the provisions of this Act,
  - (a) The Central Adjudicatory Authority shall sit at New Delhi...
  - (b) The State Adjudicating Authorities shall ordinarily sit at the State Capitals;
- (6) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.

Provided that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.

- (7) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed.

Provided that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.

- (8) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government or the State Governments, as the case may be, shall appoint another person in accordance with the provisions of this Act to fill the vacancy, and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.
- (9) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government or the State Government, as the case may be, resign his office:

Provided that, the Chairperson or any other Member shall, unless he is permitted by the Central or State Government to relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his

successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (10) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government or the State Government, as the case may be, after giving necessary opportunity of being heard.
- (11) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in accordance with the provisions of this act to fill such vacancy, enters upon his office.
- (12) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (13) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

#### **48. Staff of the adjudicating authority**

- (1) The Central Government shall provide the Central Adjudicating Authority, and the State Governments shall provide the State Adjudicating Authorities, with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees of the Adjudicating Authority shall be such as may be prescribed.

#### **49. Power regarding summons, production of documents and evidence**

- (1) The Central Adjudicating Authority and State Adjudicatory Authorities shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely
  - (a) Discovery and inspection;
  - (b) Enforcing the attendance of any person, including any officer of a Clinical establishment or a health information exchange and examining him on oath;
  - (c) Compelling the production of records;
  - (d) Receiving evidence on affidavits;



- (e) Issuing commissions for examination of witnesses and documents; and
  - (f) Any other matter which may be prescribed by the Central Government.
- (2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or make statements, and produce such documents as may be required.
- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

**50. Civil court not to have jurisdiction**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Central Adjudicatory Authority or the State Adjudicatory Authority is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**51. Appeal to High Court**

- (1) Any person aggrieved by any decision or order of the Central Adjudicatory Authority may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Adjudicatory Authority to him on any question of law or fact arising out of such order.
- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

<p>CHAPTER VII</p> <p>MISCELLANEOUS PROVISIONS</p>
--

**52. Act to supersede any other law**

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health data' hereunder.

**53. Power of the Central Government to make rules**

- (1) The Central Government may, by notification in the Official Gazette, make rules for the purposes of carrying out the provisions of this Act.

- (2) Every Rule made by the Central government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament.

**54. Power of the State Government to make Rules –**

- (1) Subject to the other provisions of this Act, the State Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act;
- (2) Every Rule made by the State government under this Act shall as soon as may be after its made, be placed in each House of the State Legislature, where there are two houses.

**55. Removal of difficulty by the government**

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.
- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

\*\*\*

**Schedule I****Personally Identifiable Information**

- (iv) Name
- (v) Address
- (vi) Date of Birth
- (vii) Telephone Number
- (viii) Email Address
- (ix) Password
- (x) Financial information such as bank account or credit card or debit card or other payment instrument details;
- (xi) Physical, physiological and mental health condition;
- (xii) Sexual orientation;
- (xiii) Medical records and history;
- (xiv) Biometric Information;
- (xv) Vehicle number
- (xvi) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL').

New Issue – we should not disallow direct sharing of identifiable data for direct patient care between two hospitals.

772665/2018/US(SKP)-e-HEALTH



LAV AGARWAL, A.S.  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail : alav@ias.nic.in



सत्यमेव जयते

भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011  
Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No.Z-18015/23/2017-eGov  
Dated: 21<sup>st</sup> December, 2017

Dear Sir,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders. Salient features of draft act include:

- Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to).
- Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- Providing for establishment of Digital Health Information Exchanges; and
- Framework to provide for civil and criminal remedies for data breach.

772665/2018/US(SKP)-e-HEALTH

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act to your ministry for seeking comments and suggestion on the draft act before putting this up in public domain for feedback.

With *sincere regards,*

Yours sincerely,



(Lav Agarwal)

**Shri Ajay Prakash Sawhney**

Secretary,

Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi, 110003



772665/2018/US(SKP)-e-HEALTH



LAV AGARWAL IAS  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011

Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No.Z-18015/23/2017-eGov

Dated: 21<sup>st</sup> December, 2017

Dear Sir,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders. Salient features of draft act include:

- Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to).
- Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- Providing for establishment of Digital Health Information Exchanges; and
- Framework to provide for civil and criminal remedies for data breach.

772665/2018/US(SKP)-e-HEALTH

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act to your ministry for seeking comments and suggestion on the draft act before putting this up in public domain for feedback.

With *sincere regards,*

Yours sincerely,



(Lav Agarwal)

Shri Rajiv Gauba  
Secretary,  
Ministry of Home Affairs  
North Block, Central Secretariat  
New Delhi-110001

# **Digital Information Security in Healthcare, Act**

***[Draft for Public Consultation]***

**November, 2017**

**Ministry of Health & Family Welfare,  
Government of India**



INDEX

SL. NO.	PARTICULARS	PAGE NO.
1	CHAPTER I – PRELIMINARY	2
2	CHAPTER II - NATIONAL ELECTRONIC HEALTH AUTHORITY	6
	STATE ELECTRONIC HEALTH AUTHORITIES	
	HEALTH INFORMATION EXCHANGES	
3	CHAPTER III – POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES	13
4	CHAPTER IV - DATA OWNERSHIP, SECURITY AND STANDARDIZATION	
5	CHAPTER V- DIGITAL HEALTH DATA BREACH AND CONSEQUENCES	24
6	CHAPTER VI- ADJUDICATING AUTHORITY	27
7	CHAPTER VII- MISCELLANEOUS PROVISIONS	31

Digital Information Security in Healthcare Act (INSERT YEAR)

An Act to provide for establishment of National and State eHealth Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data and such other matters related and incidental thereto.

BE IT ENACTED by Parliament in (insert year) of the Republic of India as follows:

CHAPTER I  
PRELIMINARY

1. SHORT TITLE, EXTENT

- (1) This Act may be called as Digital Information Security in Healthcare Act (DISHA) (insert year).
- (2) It extends to whole of India except the State of Jammu and Kashmir.

2. COMMENCEMENT AND APPLICATION

- (1) This Act shall come into force on such date as the Central Government may, by notification, appoint; and different dates may be appointed for different States and for different provisions of this Act.

3. DEFINITIONS

- (1) In this Act, unless the context otherwise requires,
  - (a) ‘Anonymization’ means the process of permanently deleting all personally identifiable information from an individual’s digital health data.
  - (b) ‘Breach’ shall have the same meaning as assigned to it in Section 37 of this Act.
  - (c) ‘Consent’ means expressed informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.

Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.

- (d) ‘De-identification’ means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual’s digital health data in a manner that

eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.

- (e) **‘Digital Health Data’** means an electronic record of health-related information about an individual and shall include the following:
  - (i) Information concerning the physical or mental health of the individual;
  - (ii) Information concerning any health service provided to the individual;
  - (iii) Information concerning the donation by the individual of any body part or any bodily substance;
  - (iv) Information derived from the testing or examination of a body part or bodily substance of the individual;
  - (v) Information that is collected in the course of providing health services to the individual; or
  - (vi) Information relating to details of the clinical establishment accessed by the individual.
- (f) **‘Entity’** includes any of the following, not being a clinical establishment:
  - (i) An individual;
  - (ii) A company;
  - (iii) A department of the Central or State Government;
  - (iv) A firm;
  - (v) An association of persons or a body of individuals, whether incorporated or not, in India or outside India; or
  - (vi) Any corporation established by or under any Central, State or Provincial Act or a Government company as defined in section 2(45) of the Companies Act, 2013;
  - (vii) Any body corporate incorporated by or under the laws of a country outside India;
  - (viii) A co-operative society registered under any law relating to cooperative societies;
  - (ix) A local authority;
  - (x) Every artificial juridical person, not falling within any of the preceding sub-clauses;
- (g) **‘Guardian’** means a guardian recognised under any law for the time being in force.
- (h) **‘Health Information Exchange’** means a health information exchange as established under this Act.

- (i) **‘Clinical Establishment’** means (i) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicines established and administered or maintained by any person or body of persons, whether incorporated or not; or (ii) a place established as an independent entity or part of an establishment referred to in sub-clause (i), in connection with the diagnosis where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not, and shall include a clinical establishment owner, controlled or managed by
- the Government or a department of the Government;
  - a trust, whether public or private;
  - a corporation (including a society) registered under a Central, Provincial or State Act, whether or not owned by the Government;
  - a local authority;
  - a single doctor,
- but does that include the clinical establishments owned, controlled or managed by the Armed Forces.  
Explanation: For the purpose of this clause, “Armed Forces” means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)
- (j) **‘Owner’** means an individual whose digital health data is generated and processed under this Act.
- (k) **‘Personally Identifiable Information’** means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I.
- (l) **‘Prescribed’** shall mean rules prescribed by the Central Government or the State Governments as the case may be.
- (m) **‘Relative’** with reference to the owner, means—
- spouse of the owner;
  - parents of the owner;
  - brother or sister of the owner;

- (iv) brother or sister of the spouse of the owner;
  - (v) brother or sister of either of the parents of the owner;
  - (vi) in the absence of any of the relatives mentioned at sub-clauses (i) to (v), any lineal ascendant or descendant of the owner;
  - (vii) in the absence of any of the relatives mentioned at sub-clauses (i) to (vi), any lineal ascendant or descendant of the spouse of the owner;
- (n) **‘Data Security’** refers directly to protection of digital health data, and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.
- (o) **‘Sensitive health-related information’** means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, Human Immunodeficiency Virus status, Sexually Transmitted Infections treatment, and abortion.
- (p) **‘serious breach’** shall have the same meaning as assigned to it in Section 38 of this Act.
- (q) **‘Specified’** shall mean as specified by National eHealth Authority of India or State eHealth Authority, as the case may be.
- (r) **“need to know basis”** means the access to digital health data by a specific person for a specific and lawful purpose that is necessary for that purpose or to carry out that function.

CHAPTER II  
NATIONAL ELECTRONIC HEALTH AUTHORITY OF INDIA,  
STATE ELECTRONIC HEALTH AUTHORITIES AND  
HEALTH INFORMATION EXCHANGES

**4. National Electronic Health Authority of India (NeHA)**

- (1) The Central Government shall establish for the purposes of this Act, a National Electronic Health Authority of India, by Notification in the

Official Gazette, which may be referred to as NeHA in its abbreviated form.

- (2) The National Electronic Health Authority of India, shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the Central Government, specifies a separate date in the same Notification.

#### **5. Composition of National Electronic Health Authority of India**

- (1) National Electronic Health Authority of India shall consist of the following members, to be appointed by the Central Government by Notification, namely:
  - (a) A full time Chairperson;
  - (b) A member -secretary; equivalent to the rank of Joint Secretary to the Government of India
  - (c) Four full-time members to be appointed by the Central Government:
    - (i) One from health informatics;
    - (ii) One from public health;
    - (iii) One from law; and
    - (iv) One from public policy
  - (d) Four ex-officio members, not less than the rank of Joint Secretary to the Government of India to be appointed by the Central Government:
    - (i) One from Ministry of Electronics and Information Technology;
    - (ii) One from Ministry of Panchayati Raj/ Ministry of Women & Child Development;
    - (iii) One from Directorate General of Health Services; and
    - (iv) One from Ministry of Law and Justice
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
  - (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Fifteen years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.

Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.

- (3) The National Authority shall be a body corporate with the name specified by the Central Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and

dispose of property and to contract, and may, by the said name, sue or be sued.

#### **6. National Executive Committee**

- (1) The Central Government shall, immediately after the notification under sub-section (1) of Section 4, constitute a National Executive Committee to assist the National Authority in the performance of its functions under this Act.
- (2) The National Executive Committee shall consist of the following members, namely:-
  - (a) Additional Secretary/Joint Secretary, ehealth as Chairperson;
  - (b) Deputy Commissioner/Assistant Commissioners as members;
  - (c) Director/Deputy Secretary as member; and
  - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the National Executive Committee may invite any other officer of the Central Government or a State Government for taking part in any meeting of the National Executive Committee and shall exercise such powers and perform such functions as may be prescribed by the Central Government in consultation with the National Authority.
- (4) The procedure to be followed by the National Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the Central Government.

#### **7. State Electronic Health Authorities**

- (1) Every State Government shall, as soon as may be after the issue of the notification under sub-section (1) of section 4, by notification in the Official Gazette, establish a State Electronic Health Authority, which may be referred to as SeHA in its abbreviated form.
- (2) The State Electronic Health Authority shall come into force on the same day of Notification as referred to in sub-section (1) above, unless the State Government, specifies a separate date in the same Notification.

#### **8. Composition of State Electronic Health Authorities**

- (1) State Electronic Health Authority shall consist of the following members, to be appointed by the State Government by Notification, namely:
  - (a) A full time Chairperson;
  - (b) Secretary in-charge of State Health Department or equivalent as member-secretary;
  - (c) Three full-time members to be appointed by the State Government:
    - (i) One from health informatics;
    - (ii) One from public health; and
    - (iii) One from law

- (d) Three ex-officio members to be appointed by the State Government:
  - (i) Director, State Health Services;
  - (ii) One from State Information Technology department; and
  - (iii) One from State Law department
- (2) Without prejudice to anything stated above, the Chairperson shall have the following qualifications:
  - (a) Be not more than sixty-five years of age;
  - (b) Be person of ability, integrity and standing; and have adequate knowledge and expertise of at least Twelve years in any of the following areas or a combination thereof:
    - (i) Information Technology (IT);
    - (ii) Health Informatics; or
    - (iii) Public Health; or
    - (iv) Law; or
    - (v) Public policy.

Provided that, to be appointed as Chairperson, the person shall additionally have demonstrable qualities of leadership, institution building.
- (3) The State Authority shall be a body corporate with the name specified by the State Government in the notification under sub-section (1), having perpetual succession and a common seal with power, subject to the provisions of this Act, to acquire, hold and dispose of property and to contract, and may, by the said name, sue or be sued.

## 9. State Executive Committee

- (1) The State Government shall, immediately after issue of notification under sub-section (1) of section (7), constitute State Executive Committee to assist the State Authority in the performance of its functions, under this Act.
- (2) The State Executive Committee shall consist of the following members, namely:—
  - (a) The Secretary Health, as the Chairperson;
  - (b) Director, Health Services as member;
  - (c) Deputy Secretary ehealth as member; and
  - (d) Supported by consultants and ehealth section.
- (3) The Chairperson of the State Executive Committee shall exercise such powers and perform such functions as may be prescribed by the State Government and such other powers and functions as may be delegated to him by the State Authority.
- (4) The procedure to be followed by the State Executive Committee in exercise of its powers and discharge of its functions shall be such as may be prescribed by the State Government.

## 10. Term of Office of Chairperson & other members of National and State Authorities



- (1) The Chairperson and members of the National Authority, shall hold office for a term of three years, as the Central Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (2) The chairperson and members of the State Authority, shall hold office for a term of three years, as the State Government may notify in this behalf, from the date on which they enter upon their offices or until they attain the age of sixty-five, whichever is earlier.
- (3) The Chairperson and other Members, appointed as per sub-section (1) of section 5 and sub-section (1) of section 8, are eligible for reappointment for another term; provided such reappointed Chairperson or Member does not exceed sixty-five years of age.

#### **11. Salary, allowance, benefits and service conditions etc.,**

- (1) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the National Authority, shall be such as may be prescribed by the Central Government.
- (2) The salary or allowances or other benefits payable to and the other terms and conditions of service of the Chairperson and full-time members of the State Authorities, shall be such as may be prescribed by the State Governments.
- (3) Notwithstanding anything stated in sub-section (1) and (2) above, the salary, allowances and other conditions of service of the Chairperson or of a member shall not be varied to his disadvantage after his appointment.

#### **12. Reconstitution of the National and State Authorities**

- (1) Any vacancy caused to the office of the Chairperson or any other member of the National & State Authority shall be filled up by the Central Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (2) Any vacancy caused to the office of the Chairperson or any other member of the State Authority shall be filled up by the State Government, immediately or in any case, not exceeding a period of three months from the date on which such vacancy occurs.
- (3) In the event of vacancy in the office of the Chairperson of the National or State Authority, the senior most person, from amongst the full time members, shall act as the Chairperson, till the vacancy is filled.
- (4) No act or proceeding of the National or State Authority shall be invalid merely by reason of-
  - (a) Any vacancy in, or any defect in the constitution of the Authority; or
  - (b) Any defect in the appointment of a person acting as a member of the Authority; or

- (c) Any irregularity in the procedure of the Authority not affecting the merits of the case.

### **13. Temporary association of persons with National or State Authorities for particular purposes –**

- (1) The National Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (2) A State Authority may associate with itself in such manner, and for such purposes, as may be prescribed, any person or Organisation, whose assistance and advice it may desire to obtain in performing any of its functions under this Act.
- (3) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall have a right to take part in the discussions of the Authority relevant to that purpose, but shall not have a right to vote at a meeting of the Authority, and shall not be a member for any other purpose.
- (4) A person associated with the National Authority or State Authorities, as the case may be, under sub-section (1) or (2) for any purpose, shall be paid such fees and allowances, for attending its meetings and for attending to any other work of the Authority, as may be prescribed.

### **14. Officers and Other Employees of the National and State Authorities**

- (1) The National Authority, in consultation with Central Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (2) The State Authority, in consultation with the State Government, may appoint officers and such other employees, as it considers necessary for the efficient discharge of its functions under this Act.
- (3) The salary and allowances payable to; and the other conditions of service of the officers and other employees of the National or State Authority appointed under sub-section (1) and (2) shall be such as may be prescribed.

### **15. Meetings**

- (1) The National Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (2) The State Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be prescribed by Central Government by Rules under this Act.
- (3) The chairperson of the National or State Authority, if unable to attend a meeting, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

**16. Disqualifications**

- (1) A person shall be disqualified for appointment as Chairperson or member of the National Electronic Health Authority or a State Electronic Health Authority, if he/she –
  - (i) Has been convicted and sentenced to imprisonment for an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (ii) Is an undercharged insolvent; or
  - (iii) Has been removed or dismissed from the service of the Government or a body corporate owned or controlled by the Government; or
  - (iv) Has in the opinion of the Central Government, such financial or other interest as is likely to affect prejudicially the discharge by him of his functions as a member; or
  - (v) Has such other disqualification as may be prescribed by the Central Government.

**17. Resignation, removal of chairperson or member of the National or State Authorities**

- (1) The Chairperson or full time member of the National Authority appointed under sub-section (1) of section 5 and the Chairperson or full time member of a State Authority appointed under sub-section (1) of section 8:
  - (a) May relinquish his/her office by submitting the resignation in writing to the Central Government or the State Government as the case may be; or
  - (b) May be removed from his/her office in accordance with the provisions of section 18.

**18. Removal in certain circumstances**

- (1) The Central Government or the State Government, may remove from office the Chairperson or any full-time member of the National or State Authority, who –
  - (a) Has been adjudged as an insolvent; or
  - (b) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
  - (c) Has become physically or mentally incapable of discharging his or her functions; or
  - (d) Has acquired such financial or other interest as is likely to affect prejudicially his or her functions as the Chairman or member; or
  - (e) Has so abused his/her position as to render his or her continuance in office prejudicial to the public interest.
- (2) No such member or Chairperson shall be removed from his/her office under clause (d) or clause (e) of sub-section (1) above, unless he/she has been given a reasonable opportunity of being heard in the matter.

**19. Health Information Exchanges**

- (1) The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act
- (2) No entity shall function as a Health Information Exchange unless established as such by the central Government

**20. Management of Health Information Exchange**

- (1) All Health Information Exchanges shall conduct and carry out their affairs strictly as per the norms, standards or protocols specified by the National Electronic Health Authority, from time to time, or as per the Rules prescribed by the Central Government.
- (2) Without prejudice to any other stipulations of this Act, a Health Information Exchange established under section 19 shall only employ such skilled personnel for management of its affairs as may be specified by the National Electronic Health Authority.
- (3) Conditions with respect to periodical reports, annual reports and direct inquiries may be such as may be prescribed by the Central Government.

**21. The Chief Health Information Executive and his functions**

- (1) The Health Information Exchange shall have a Chief Health Information Executive, abbreviatedly referred to as CHIE, who shall possess such qualifications and experiences as may be prescribed by the Central Government as rules under this Act;
- (2) The Chief Health Information Executive as appointed under sub-section (1) above, shall be the Chief Executive Officer and also the data controlling authority of the Health Information Exchange, and be responsible for all routine and day-to-day affairs, and in particular:
  - (a) Ensure the day-to-day affairs of the Health Information Exchange runs smoothly and as per the objectives and norms of this Act.
  - (b) Access, and process the digital health care data transmitted by the Clinical Establishments to further transmit the digital health care data, whenever required, in accordance with norms prescribed by the National Electronic Health Authority of India.
  - (c) Take appropriate measures to maintain, secure and protect the digital health care data as prescribed by the National Digital Health Authority of India.
  - (d) Notify the data breach to the owner and such other concerned.
  - (e) Store the digital health care data in prescribed mode in all situations.

CHAPTER III  
POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES

**22. Powers and functions of National Electronic Health Authority of India**

- (1) The National Electronic Health Authority of India in order to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Formulate standards, operational guidelines and protocols for the generation, collection, storage and transmission of the digital health data for the purposes of this Act, applicable to:
    - (i) Clinical establishments generating and collecting digital health data for their own use or for further transmission to the health information exchanges;
    - (ii) Health information exchanges storing and transmitting digital health data to clinical establishments, or to other health information exchanges, or to State Electronic Health Authority, or the National Electronic Health Authority;
    - (iii) Any other entity having custody of any digital health data;
    - (iv) State Electronic health Authority and the National Electronic Health Authority;
  - (b) To ensure data protection and prevent breach or theft of digital health data, establish data security measures for all stages of generation, collection, storage and transmission of digital health data, which shall at the minimum include access controls, encrypting and audit trails;
  - (c) Conduct periodical investigations to ensure compliance with the provisions of this Act and any rules, regulations, standards or protocols hereunder by health information exchanges;
  - (d) Notify and mandate the health information exchanges, in case of failure to comply with the provisions of this Act;
  - (e) To lay down protocol for transmission of digital health data to and receiving it from other countries;
  - (f) Collaborate and work with Standardization Testing and Quality Certification of digital health care system, by establishing necessary norms and institutions, including collaborating with existing institutions;
  - (g) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (g) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed

**23. National Authority's power of oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the National Electronic Health Authority or its representative, shall have the right to inspect all such records; or access the premises, including virtual premises of the health information exchange or exchanges at any time.

**Provided** that National Electronic Health Authority, while accessing such records or accessing either the physical or virtual premises of health information exchanges, shall bear in mind that no or least possible hindrance is caused to the normal working of the health information exchange.

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the National Electronic Health Authority to generally discharge its functions under this Act, shall direct a health information exchange or class of health information exchanges, or all health information exchanges as the case may be, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the National Electronic Health Authority, shall be binding upon the health information exchange or health information exchanges.

**24. Powers and Functions of State Electronic Health Authorities**

- (1) The State Electronic Health Authority to ensure confidentiality and privacy of digital health data shall have the following powers and functions:
  - (a) Ensure that the clinical establishments and other entities in the state collect, store, transmit and use digital health data as per the provisions of this Act and the standards, protocols and operational guidelines issued by the National Electronic Health Authority, from time to time;
  - (b) Conduct investigations to ensure compliance with the provisions of this Act;
  - (c) Notify and mandate the clinical establishments and other entities, in case of failure to comply with the provisions of this Act;
  - (d) Carry out all such incidental activities in consonance with all above powers and functions enumerated in sub-section (a) to (c) above.
- (2) Perform such other functions and exercise such other powers as may be prescribed by the Central Government.

**25. State Authority's power of Oversight, inspection, investigation and issuance of directions etc.**

- (1) To carry out all or any of the powers and functions enumerated in Section 22, the State Electronic Health Authority, or its representative, shall have the right to inspect all such records; or access the premises including virtual premises, of a Clinical establishment or other entities at any time.

**Provided** that State Electronic Health Authority while accessing such records or accessing the physical premises of Clinical establishments, shall bear in mind that no or least possible hindrance is caused to the normal working of the clinical establishment

- (2) Without prejudice to sub-section (1) above, for the purpose of enabling the State Electronic Health Authority to generally discharge its functions under this Act, it shall direct a clinical establishment or a class of clinical establishments, or all clinical establishments as the case may be, or entities, to submit such records or file such returns within such time and in such manner as specified from time to time.
- (3) All directions under this section issued by the State Digital Health Authority are binding upon the clinical establishment or clinical establishments and entities as the case may be.

**26. Power of Civil Court –** Notwithstanding anything contained in any other law for the time being in force, the National Authority while exercising the powers under section 23 and the State Authorities while exercising the powers under section 25, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-

- (a) summoning and enforcing the attendance of witnesses and examining them on oath;
- (b) discovery and production of any document;
- (c) receiving evidence on affidavit;
- (d) requisitioning any public record or copy thereof from any court or office;
- (e) issuing commissions for examination of witnesses or documents;
- (f) any other matter which may be prescribed

**27. Power to give directions –**

- (1) In the performance of its functions under this Act, -
  - (a) The National Authority shall be bound by such directions in writing as the Central Government may give to it;
  - (b) Every State Authority shall be bound by such direction in writing as the National Authority or the State Government may give to it;

*Provided that* where a direction given by the State Government is inconsistent with the direction given by the National Authority, the matter shall be referred to the Central Government for its decision, which shall be final.

- (c) Every Health Information Exchange shall be bound by such directions in writing as the National Authority may give to it;
- (d) Every Clinical Establishment shall be bound by such directions in writing as the State Authority may give to it.

#### CHAPTER IV

##### DATA OWNERSHIP, SECURITY AND STANDARDIZATION

#### **28. The rights of the owner of digital health data**

- (1) An owner shall have the right to privacy, confidentiality, and security of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.
- (2) An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 29 of this Act.
- (3) An owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data.
- (4) An owner shall have the right to refuse consent to the access or disclosure of his or her digital health data, and if refused it shall not be disclosed, subject to the exceptions provided in Section 33 of the Act.
- (5) An owner of the digital health data shall have the right that the digital health data collected must be specific, relevant and not excessive in relation to the purpose or purposes for which it is sought;
- (6) An owner of the digital health data shall have the right to know the clinical establishments or entities which may have or has access to the digital health data, and the recipients to whom the data is transmitted or disclosed;
- (7) The owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any Clinical Establishment/Entity;
- (8) The owner of the digital health data shall have, subject to sub-section (1) to (3) above:
  - (a) The right to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data, in the prescribed form as may be notified by the National Electronic Health Authority;
  - (b) The right to require their explicit prior permission for each instance of transmission or use of their digital health data in



- an identifiable form, through such means as may be prescribed by the Central Government;
- (c) The right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 34 of the Act;
- (d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;
- (e) The right to prevent any transmission or disclosure of any sensitive health related data that is likely to cause damage or distress to the owner;
- (f) The right not to be refused health service, if they refuse to consent to generation, collection, storage, transmission and disclosure of their health data;
- (g) The right to seek compensation for damages caused by a breach of digital health data.

**29. Purposes of collection, storage, transmission and use of the digital health data**

- (1) Digital health data may be generated, collected, stored, and transmitted by a clinical establishment and; collected, stored and transmitted by health information exchange, for the following purposes:
  - (a) To advance the delivery of patient centered medical care;
  - (b) To provide appropriate information to help guide medical decisions at the time and place of treatment;
  - (c) To improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;
  - (d) To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;
  - (e) To facilitate health and clinical research and health care quality;
  - (f) To promote early detection, prevention, and management of chronic diseases;
  - (g) To carry out public health research, review and analysis, and policy formulation;
  - (h) To undertake academic research and other related purposes

Provided that personally identifiable information may only be used for the purposes of direct care of the owner of the data, as specified in clauses (a) to (c) of sub-section (1), subject to provisions of section 28, to the extent considered necessary, and in the best interest of the owner

Provided further that for public health related purposes mentioned in clauses (d) to (h) of sub-section (1), only de-identified or anonymized data shall be used, in the manner as may be prescribed under this Act.

- (2) Digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (c) of Sub-Section (1).
- (3) Digital health data shall not be used for any other purpose, except in accordance with the provisions of this Act.

Provided that the digital health data shall be used only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to use the information.

- (4) There shall be no access to, or disclosure of personally identifiable information, except in accordance with the provisions of this Act.

Provided that the digital health data shall be accessed or disclosed only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to access or disclose the information.

- (5) Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government.

Explanation: Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim.

Provided that for the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates

### **30. Collection of health data**

- (1) No health data shall be collected, for the purposes of conversion to digital health data, by any clinical establishment, or any other entity in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may, by consent from the owner, recorded in the form and manner as may be prescribed under this Act, lawfully collect the required health data, after informing the owner of the following:

- (a) The rights of the owner as laid down in this Act, including the right to refusal to give consent to the generation and collection of such data;
- (b) The purpose of collection of such health data;
- (c) The identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format;
- (d) The identity of the recipients who may have access to such digital health data on a need to know basis
- (3) A clinical establishment or any other entity, shall furnish a copy of the consent form to the owner.
- (4) Any other entity that collects any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data.
- (5) Without prejudice to the above sub-section (2), when an individual is incapacitated or incompetent to provide consent, either due to physical or mental incapacity, the clinical establishment may collect health data by obtaining proxy consent from a nominated representative, relative, care giver or such other person, as may be prescribed under this Act, and who has the legal capacity to consent.

Provided that where the individual has regained his or her capacity to give or refuse consent for the collection of his or her health data by the clinical establishment, he or she shall have the option to seek withdrawal of proxy consent and obtaining his or her own consent for collection of such health data, in such form and manner as may be prescribed by the National Electronic Health Authority of India.

- (6) Where a person is a minor and it is in the best interest of the minor, proxy consent can be obtained by the minor's legal guardian, or representative.

Provided that upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.

### **31. Ownership of digital health data**

- (1) The digital health data generated, collected, stored or transmitted shall be owned by the individual whose health data has been digitised;
- (2) A clinical establishment or Health Information Exchange shall hold such digital health care data referred to in sub-section (1) above in trust for the owner;
- (3) Any other entity who is in custody of any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data;
- (4) Notwithstanding anything stated in the above sub-sections (1) to (3), the medium of storage and transmission of digital health data shall be

owned by the clinical establishment or health information exchange, as the case may be.

### 32. Storing of digital health data

- (1) No digital health data shall be stored by any clinical establishment or entity or health information exchange in any manner, except in accordance with the provisions of this Act.
- (2) The clinical establishment or health information exchange, as the case may be, shall hold all digital health data, on behalf of National Electronic Health Authority; and such data be used for such purposes as stated in Section 29, without compromising the privacy or confidentiality of the owner, and security of such data.
- (3) The digital health data vested with the National Electronic Health Authority as per sub-section 2 above, shall be stored and may be transmitted or used in such form and manner as may be prescribed by the National Electronic Health Authority.

### 33. Transmission of data

- (1) No digital health data shall be transmitted by a clinical establishment or health information exchange, or any other entity, as the case may be, in any manner, except in accordance with the provisions of this Act.
- (2) A clinical establishment may transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the clinical establishment.

**Provided** that for such secure, encrypted and instantaneous transmission of digital health data as referred in sub-section (2), the National Electronic Health Authority of India shall prescribe appropriate standards for physical, administrative and technical measures, keeping in mind the privacy and confidentiality of the owner, by notification

- (3) The digital health data shall be transmitted by a clinical establishment or entity or health information exchange only upon the consent of the owner, after being informed of the rights of the owner under Section 28, and the specific purposes of collection of such data under Section 29.
- (4) A health information exchange shall maintain a register in such form and manner as may be prescribed by the Central Government, containing all details of the transmission of the digital health data between a clinical establishment and health information exchange, and between health information exchanges *inter se*.

### 34. Access to digital health data

- (1) No digital health data collected, stored or transmitted by a clinical establishment or health information exchange, as the case may be,

shall be accessed by any person, except in accordance with the provisions of this Act.

- (2) The digital health data collected or stored or transmitted by a clinical establishment or health information exchange, as the case may be, may be accessed by the clinical establishment, on a need to know basis, in such form and manner as may be prescribed under this Act.
- (3) The government departments through their respective Secretaries, may submit request for digital health data in de-identified/anonymized form, to the National Electronic Health Authority, in the form and manner specified by the Authority, subject to provisions of clauses (d) to (h) of sub-section (1) of section 29 of this act.

Provided that the National Electronic Health Authority of India may prescribe any other class of persons who may access digital health data, which is anonymized, for the purposes stated in clause (d) to (h) of sub-section (1) of section 29 of the Act.

- (4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for administration of justice, such access may be granted to an investigating authority only with the order of the competent court;
- (5) The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India.
- (6) In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified;
- (7) In case of an emergency, the relatives of the owner may have access to such data for the purpose of correct treatment of the owner, subject to such conditions as may be prescribed under this Act.
- (8) In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Electronic Health Authority of India.

Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.

Provided further that in case of death of the owner, the National Electronic Health Authority, shall use the digital health data only in anonymized form.

- (9) All clinical establishments and health information exchanges shall maintain a register in a digital form to record the purposes and usage of digital health data accessed within the meaning of this Section, in such form and manner, as may be specified by the National Electronic Health Authority.

### **35. Duty to maintain privacy and confidentiality of digital health data**

- (1) A clinical establishment, health information exchange, State Electronic Health Authority and the National Electronic Health Authority, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner;
- (2) Any other entity, which has generated and collected digital health data, shall be duty bound to protect the privacy, confidentiality, and security of the digital health data of the owner.
- (3) The privacy, confidentiality and security of digital health data shall be ensured by taking all necessary physical, administrative and technical measures, that may be prescribed or specified, to ensure that the digital health data, collected, stored and transmitted by them, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.
- (4) Without prejudice to the above provisions, a clinical establishment or health information exchange shall ensure through regular training and oversight that their personnel comply with the security protocols and procedures as may be prescribed or specified under this act.
- (5) A clinical establishment, or a health information exchange, shall provide notice immediately, and in all circumstances not later than three working days to the owner, in such manner as may be prescribed under this Act, in case of any breach or serious breach of such digital health data.

### **36. Procedure for rectification of digital health data**

- (1) An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed under this Act.
- (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.

## CHAPTER V OFFENCES AND PENALTIES

### **37. Breach of digital health data**

- (1) Digital health data is said to be breached, if:
  - (a) any person generates, collects, stores, transmits or discloses digital health information in contravention to the provisions of Chapter II of this Act; or

- (b) Any person does anything in contravention of the exclusive right conferred upon the owner of the digital health data; or
  - (c) Digital health data collected, stored or transmitted by any person is not secured as per the standards prescribed by the Act or any rules thereunder; or
  - (d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data.
- (2) Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place.

### **38. Serious breach of digital health data:**

- (1) A serious digital health data breach shall be said to have taken place, if:
- (a) A person commits a breach of digital health data intentionally, dishonestly, fraudulently or negligently; or
  - (b) Any breach of digital health data occurs, which relates to information which is not anonymised or de-identified; or
  - (c) A breach of digital health data occurs where a person failed to secure the data as per the standards prescribed by the Act or any rules thereunder; or
  - (d) Any person uses the digital health data for commercial purposes or commercial gain; or
  - (e) An entity, clinical establishment or health information exchange commits breach of digital health data repeatedly;

Explanation: The terms “dishonestly” and “fraudulently” shall have the same meaning as assigned to them under the Indian Penal Code, 1860

- (2) Any person who commits a serious breach of health care data shall be punished with imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.

Provided that, any fine imposed as part of sub-section (2) may be provided to the individual whose data is breached, by the Court, as it deems fit as compensation.

### **39. Compensation for serious breach of digital health information**

- (1) A person or an entity committing a serious breach of digital health information shall be liable to pay damages by way of compensation to the owner of the digital health data in relation to which the breach took place.
- (2) Where any compensation has been awarded under sub-section (2) of section 37, it shall be taken into account when determining the claim made by the person affected.

**40. Penalty for failure to furnish information, return or failure to observe rules and directions, etc.,**

- (1) If any person required under this Act or any rules made thereunder, fails to furnish any information or document or books or returns or reports etc., within the time specified, to National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (2) Any person required under this Act or any rules made thereunder fails to comply, within the time specified, with directions issued by the National Electronic Health Authority, or the State Electronic Health Authority, as the case may be, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees;
- (3) Any person which is required under this Act or any rules made thereunder, after having been called upon by the National Electronic Health Authority in writing, or the State Electronic Health Authority, as the case may be, to redress the grievances of owners of digital healthcare data, fails to redress such grievances within the time specified, shall be liable to a penalty of minimum one lakh of rupees and rupees ten thousand for each day during which such failure continues subject to a maximum of one crore rupees.

**41. Obtaining the digital health information of another person**

Whoever, fraudulently or dishonestly, obtains the digital health information of another person, which he is not entitled to obtain under the Act from a person or entity storing such information shall be punished with imprisonment for a term which shall extend up to one year or fine, which shall be not less than one lakh rupees; or both.

**42. Data theft**

Whoever intentionally and without authorization acquires or accesses any digital health data shall be punished with imprisonment for a term, which shall extend from three years up to five years or fine, which shall be not less than five lakh rupees; or both.

**43. Cognizance of offences by court**

- (1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made thereunder, save on complaint made by the Central Government, State Government, the National Electronic Health Authority of India, State Electronic Health Authority, or a person affected.
- (2) No Court inferior to that of a Court of Sessions shall try any offence punishable under sections 38, 41 and 42 of this Act.



**44. Offences by companies**

- (1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time when the contravention was committed, was in charge of and was responsible to the company, for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the contravention, and shall be liable to be proceeded against and punished accordingly.

**Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the commission of such contravention.

- (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer of the company shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

**Explanation 1.**— For the purpose of this Section —

- (a) **“company”** means any body corporate and includes a clinical establishment, entity, firm or other association of individuals; and
- (b) **“director”** in relation to
- (i) a firm, means a partner in the firm;
  - (ii) any association of persons or a body of individuals, means any member controlling the affairs thereof;

**Explanation 2.**— For the removal of doubts it is hereby clarified that a company may be prosecuted notwithstanding that the prosecution or conviction of any legal juridical person shall be contingent on the prosecution or conviction of any individual.

CHAPTER VI
------------

CENTRAL AND STATE ADJUDICATING AUTHORITIES
--

**45. Complaints to State Adjudicating Authority**

- (1) For any breach of digital health data by a clinical establishment or any entity an aggrieved person or owner may complain to the State Adjudicatory Authority in writing as may be prescribed, and seek

reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;

- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (2) or (3) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Electronic Health Authority under section 40 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.

#### **46. Complaints to the Central Adjudicating Authority**

- (1) For any breach of digital health data by a health information exchange or State Electronic Health Authority or the National Electronic Health Authority of India, an aggrieved person or owner may complain to the Central Adjudicatory Authority in writing as may be prescribed, and seek reasonable monetary compensation (damages) for the digital health data breach and consequence thereof;
- (2) No such complaints under sub-sections (1), shall be made after two years from the date of, such person or owner coming to know about the digital health data breach;
- (3) Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;
- (4) Notwithstanding anything stated in either sub-section (3) or (4) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;
- (5) Any person or entity aggrieved by the order, direction or penalties imposed by the National Electronic Health Authority under section 40 of this act, may prefer an appeal to the Central Adjudicating Authority under this Act within a period of forty-five days from the date on which a copy of the order is received.
- (6) Any person or entity or owner or State Electronic Health Authority, aggrieved by the order of the State Adjudicatory Authority may prefer an appeal to the Central Adjudicatory Authority, within 3 months from the date on which a copy of the order is received.

#### **47. Adjudicating authorities, composition, powers etc.**

- (1) The Central Government shall by Notification, appoint a Central Adjudicating Authority, and the State Governments shall by notification,

appoint State Adjudication Authorities respectively, to exercise jurisdiction, powers and authority conferred by or under this Act

- (2) The Adjudicating Authority, whether Central or State, shall consist of a Chairperson and two other members, provided that at least one of such persons shall be from the field of law.
- (3) A person shall, however, not be qualified for appointment as Member of an Adjudicating Authority –
  - (a) In the field of law, unless he:
    - (i) Is qualified for appointment as District Judge; or
    - (ii) Has been a member of the Indian Legal Service and has held a post in Grade I of the service;
  - (b) In the field of medicine, information (health) science or administration, unless he possesses such qualifications as may be prescribed by the Central Government.
- (4) The Central Government and the State Governments shall appoint the Member from the field of law, to be the Chairperson of the Central Adjudicating Authority and State Adjudicatory Authorities respectively.
- (5) Subject to the provisions of this Act,
  - (a) The Central Adjudicatory Authority shall sit at New Delhi...
  - (b) The State Adjudicating Authorities shall ordinarily sit at the State Capitals;
- (6) The Chairperson and every Member shall hold office as such for a term of five years from the date on which he enters upon his office.

Provided that no Chairperson or other Member shall hold office as such after he has attained the age of sixty-five years.

- (7) The salary and allowances payable and other terms and conditions of service of the Members shall be such as may be prescribed.

Provided that neither the salary or allowances nor the other terms and conditions of service of the Member shall be varied to his disadvantage after appointment.

- (8) If, for any reasons other than temporary absence, any vacancy occurs in the office of the Chairperson or any other Member, then the Central Government or the State Governments, as the case may be, shall appoint another person in accordance with the provisions of this Act to fill the vacancy, and the proceedings may be continued before the Adjudicating Authority from the stage at which the vacancy is filled.
- (9) The Chairperson or any other Member may, by notice in writing under his hand addressed to the Central Government or the State Government, as the case may be, resign his office:

Provided that, the Chairperson or any other Member shall, unless he is permitted by the Central or State Government to relinquish his office sooner, continue to hold office until the expiry of the three months from the date of receipt of such notice or until a person duly appointed as his

successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- (10) The Chairperson or any other Member shall not be removed from his office except by an order made by the Central Government or the State Government, as the case may be, after giving necessary opportunity of being heard.
- (11) In the event of the occurrence of any vacancy in the office of the Chairperson by reason of his death, resignation or otherwise, the senior-most Member shall act as the Chairperson of the Adjudicating Authority until the date on which a new Chairperson appointed in accordance with the provisions of this act to fill such vacancy, enters upon his office.
- (12) When the Chairperson of the Adjudicating Authority is unable to discharge his functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson of the Adjudicating Authority until the date on which the Chairperson of the Adjudicating Authority resumes his duties.
- (13) The Adjudicating Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Adjudicating Authority shall have powers to regulate its own procedure.

#### **48. Staff of the adjudicating authority**

- (1) The Central Government shall provide the Central Adjudicating Authority, and the State Governments shall provide the State Adjudicating Authorities, with such officers and employees as it may think fit.
- (2) The officers and employees of the Adjudicating Authority shall discharge their functions under the general superintendence of the Chairperson of the Adjudicating Authority.
- (3) The salaries and allowances and other conditions of service of the office and employees of the Adjudicating Authority shall be such as may be prescribed.

#### **49. Power regarding summons, production of documents and evidence**

- (1) The Central Adjudicating Authority and State Adjudicatory Authorities shall, for the purposes of this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a complaint in respect of the following matters, namely
  - (a) Discovery and inspection;
  - (b) Enforcing the attendance of any person, including any officer of a Clinical establishment or a health information exchange and examining him on oath;
  - (c) Compelling the production of records;
  - (d) Receiving evidence on affidavits;

- (e) Issuing commissions for examination of witnesses and documents; and
  - (f) Any other matter which may be prescribed by the Central Government.
- (2) All persons so summoned shall be bound to attend in person or through authorized agents, as the Adjudicating Authority may direct, and shall be bound to state the truth upon any subject respecting which they are examined or make statements, and produce such documents as may be required.
- (3) Every proceeding under this section shall be deemed to be a judicial proceeding within the meaning of Section 193 and Section 228 of the Indian Penal Code (45 of 1860).

**50. Civil court not to have jurisdiction**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Central Adjudicatory Authority or the State Adjudicatory Authority is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**51. Appeal to High Court**

- (1) Any person aggrieved by any decision or order of the Central Adjudicatory Authority may file an appeal to the High Court within sixty-days from the date of communication of the decision or order of the Adjudicatory Authority to him on any question of law or fact arising out of such order.
- (2) Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

**CHAPTER VII**  
**MISCELLANEOUS PROVISIONS**

**52. Act to supersede any other law**

- (1) The provisions of this Act shall be taken to supersede any other law for the time being in force with respect to digital medical record, digital health record or digital personal/protected health information which is being referred to as 'digital health data' hereunder.

**53. Power of the Central Government to make rules**

- (1) The Central Government may, by notification in the Official Gazette, make rules for the purposes of carrying out the provisions of this Act.

- (2) Every Rule made by the Central government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament.

**54. Power of the State Government to make Rules –**

- (1) Subject to the other provisions of this Act, the State Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act;
- (2) Every Rule made by the State government under this Act shall as soon as may be after its made, be placed in each House of the State Legislature, where there are two houses.

**55. Removal of difficulty by the government**

- (1) This Act shall be applied and construed to effectuate its general purpose to facilitate uniformity of the law/s with respect to the subject matters of this Act among all the States.
- (2) Notwithstanding the above, this Act does not restrict or limit the rights and obligations under any of the State laws or regulations, so long as the rights and obligations enumerated herein are fully complied with.
- (3) In the event of a conflict between this Act and other State or local laws or regulations, or administrative procedures, the provisions of this Act shall apply. However, the existing laws, rules and regulations, at national and State levels, shall continue to prevail to the extent of consistency with this Act and only portions thereof shall become severable and unenforceable to the extent of inconsistency with any provision of this Act.
- (4) The provisions of this Act are severable such that if any provision of this Act or its application to any person or circumstances is held invalid judicially, the invalidity shall not affect other provisions or applications of this Act which can be given effect to without the particular invalid provision or application.
- (5) Notwithstanding the above, the Governments shall undertake a comprehensive review of all the laws or provisions of laws related to health within 1 year of this Act coming into force for their compatibility with this Act.

\*\*\*

**Schedule I****Personally Identifiable Information**

- (iv) Name
- (v) Address
- (vi) Date of Birth
- (vii) Telephone Number
- (viii) Email Address
- (ix) Password
- (x) Financial information such as bank account or credit card or debit card or other payment instrument details;
- (xi) Physical, physiological and mental health condition;
- (xii) Sexual orientation;
- (xiii) Medical records and history;
- (xiv) Biometric Information;
- (xv) Vehicle number
- (xvi) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL').

New Issue – we should not disallow direct sharing of identifiable data for direct patient care between two hospitals.



**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195

T/Fax : 011-23061842

E-mail. : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011  
Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No. Z-18015/23/2017-e-Gov

Dated the: 16th January, 2018

Dear *Sir,*

Please refer to my D.O. letter of even number dated 21<sup>st</sup> December 2017 (copy enclosed) seeking comments and suggestions on the draft Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

2. Since the matter is of utmost importance, it is requested that comments and suggestion of your Ministry on the draft act may kindly be sent by 20<sup>th</sup> January, 2018 so that the same can be put up in the public domain for feedback.

With *sincere regards,*

Yours sincerely.

*(Signature)*  
(Lav Agarwal)

**Shri Rajiv Gauba**  
Secretary,  
Ministry of Home Affairs,  
North Block, Central Secretariat  
New Delhi-110001





**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail. : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011

Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No. Z-18015/23/2017-e-Gov  
Dated the: 16th January, 2018

Dear Sir,

Please refer to my D.O. letter of even number dated 21<sup>st</sup> December 2017 (copy enclosed) seeking comments and suggestions on the draft Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

2. Since the matter is of utmost importance, it is requested that comments and suggestion of your Ministry on the draft act may kindly be sent by 20<sup>th</sup> January, 2018 so that the same can be put up in the public domain for feedback.

With sincere regards.

Yours sincerely.

  
(Lav Agarwal)

**Shri A. P. Sawhney**  
Secretary,  
MeitY, Electronic Niketan,  
6, CGO Complex,  
Lodhi Road New Delhi-110003



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011

Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail. : alav@ias.nic.in

D.O. No. Z-18015/23/2017-e-Gov  
Dated the: 16th January, 2018

Dear

Please refer to my D.O. letter of even number dated 21<sup>st</sup> December 2017 (copy enclosed) seeking comments and suggestions on the draft Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

2. Since the matter is of utmost importance, it is requested that comments and suggestion of your Ministry on the draft act may kindly be sent by 20<sup>th</sup> January, 2018 so that the same can be put up in the public domain for feedback.

With

Yours sincerely.

(Lav Agarwal)

1. **Shri Rajiv Gauba**  
Secretary,  
Ministry of Home Affairs,  
North Block, Central Secretariat  
New Delhi-110001
2. **Shri A. P. Sawhney**  
Secretary, MeitY  
Electronic Niketan,  
6, CGO Complex,  
Lodhi Road New Delhi-110003



**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail. : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011  
Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No. Z-18015/23/2017-e-Gov  
Dated the: 16th January, 2018

Dear

Please refer to my D.O. letter of even number dated 21<sup>st</sup> December 2017 (copy enclosed) seeking comments and suggestions on the draft Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

2. Since the matter is of utmost importance, it is requested that comments and suggestion of your Ministry on the draft act may kindly be sent by 20<sup>th</sup> January, 2018 so that the same can be put up in the public domain for feedback.

With

Yours sincerely.

(Lav Agarwal)

1. **Shri Rajiv Gauba**  
Secretary,  
Ministry of Home Affairs,  
North Block, Central Secretariat  
New Delhi-110001

2. **Shri A. P. Sawhney**  
Secretary, MeitY  
Electronic Niketan,  
6, CGO Complex,  
Lodhi Road New Delhi-110003



No. II/21021/210/2012--ISII/M  
Government of India  
Ministry of Home Affairs  
(CIS Division/CIS-III desk)

809406  
9/2/18

North Block, New Delhi  
Date: 7<sup>th</sup> February, 2018

**OFFICE MEMORANDUM**


**Sub: Comments on draft of Digital Information Security in Healthcare Act for setting up of "National Electronic Health Authority of India" - regarding**

The undersigned is directed to refer DO No. Z-18015/23/2017-eGov dated 21.12.2017 of Ministry of Health & Family Welfare seeking comments on draft Digital Information Security in Healthcare Act (DISHA for setting up of "National Electronic Health Authority of India (NeHA)" and to state the draft Act is mainly about establishing of National Electronic Health Authority of India (NeHA), State Electronic Health Authority (SeHA), Health Information Exchanges, Central Adjudicating Authority, State Adjudicating Authorities, etc.

2. The proposed Act does not specifically mention about measures to be taken for security of sensitive medical data stored and during data transmission for exchange. Any leakage of the data can result into serious breach of privacy of individuals and health companies may take advantage of the same.

3. Further, Government of India is in the process of bringing separate Data Protection Framework which would exclusively deal with data protection issues. However, section 52 of the draft Act mentions about superseding of any other Law by DISHA with respect to digital health data. This requires deliberation among stakeholders before finalization of the draft DISHA.

Dir(e-H)  
v. signed  
Q

  
(Yogesh Pandey)  
DC(CIS-III)  
Telefax-011-2093662

To,

Shri Lav Aggarwal,  
Joint secretary,  
MO Health and Family Welfare  
Nirman Bhawan  
New Delhi-110011  
Tel:011-23061195

I/3143976/2018

D.O. No. Z-18015/23/2017-e-Gov

Dear Sir,

Please refer to my D.O. letter of even number dated 21<sup>st</sup> December 2017 (copy enclosed) seeking comments and suggestions on the draft Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

2. Since the matter is of utmost importance, it is requested that comments and suggestion of your Ministry on the draft act may kindly be sent by 10<sup>th</sup> January, 2018 subsequent to which we plan to put the draft Act in public domain for feedback.

With

Yours sincerely.

(Lav Agarwal)

1. Shri Rajiv Gauba  
Secretary,  
Ministry of Home Affairs,  
North Block, Central Secretariat  
New Delhi-110001
2. Shri A. P. Sawhney  
Secretary, MeitY  
Electronic Niketan,  
6, CGO Complex,  
Lodhi Road New Delhi-110003

I/3143977/2018

21/12/2017

Dear Sir,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of “National Electronic Health Authority of India (NeHA)”.

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders. Salient features of draft act include:

- i. Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to).
- ii. Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- iii. Providing for establishment of Digital Health Information Exchanges; and
- iv. Framework to provide for civil and criminal remedies for data breach.

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act to your ministry for seeking comments and suggestion on the draft act before putting this up in public domain for feedback.

With Regards

Lav Agarwal  
JS, e-Health

To,  
1) Secretary, MeitY  
2) Secretary, MHA

I/3143977/2018(1)

21/12/2017

Dear Sir,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of “National Electronic Health Authority of India (NeHA)”.

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a ‘sensitive data’ which deserves to be protected more than other forms of ‘personal data’. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders. Salient features of draft act include:

- i. Expressing the ‘ownership’ of ‘digital health data’ (with the person/patient to whom the digital health data belongs to).
- ii. Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- iii. Providing for establishment of Digital Health Information Exchanges; and
- iv. Framework to provide for civil and criminal remedies for data breach.

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act to your ministry for seeking comments and suggestion on the draft act before putting this up in public domain for feedback.

With Regards

Lav Agarwal  
JS, e-Health

To,  
1) Secretary, MeitY  
2) Secretary, MHA



Mail id :  
sc.rajeev72@nic.in  
rastogi.sk@nic.in  
abhishek.singh87@gov.in

For Office Use Only


Ministry of Health & Family WelfareMeta Data for Documents

Name of Division:


S.no	Item	Information to be Displayed
1.	Document title to be displayed on website	Comments on draft Digital Information Security in Healthcare, Act (DISHA)
2.	Division/Autonomous Body (Contact E-mail-id)	e-Health.
3.	Language (English)	English.
4.	Form of Document (e.g. pdf, doc, xls) (zip format not allowed)	pdf
5.	Reference URL or Detailed PDF	
6.	Validity	1 Month.
7.	Name & Email-Id of Sender	Amit Kumar (DD-eHealth), Amitkumariss34@gmail.com
8.	Section of Website, where it is to be uploaded	Programme/Reports/News & Highlights/Key Developments/Disease Alerts/Events & Announcements/Vacancies

- It is Certified that the Content have been Checked . The Content need to be following (kindly tick the appropriate option):

1. New ☒  
2. Update ☐  
3. Delete ☐

Signature:   
(अमित कुमार)  
(AMIT KUMAR)  
उप निदेशक/Deputy Director  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
Ministry of Health & Family Welfare  
भारत सरकार/Govt. of India  
नई दिल्ली/New Delhi  
Name of Nodal Officer: Amit Kumar  
Designation: Deputy Director (eHealth)  
Email-id: Amitkumariss34@gmail.com  
Contact No: 9582 861973

Contents Approved by (JS/AS)

Signature:   
Name: Lav Agarwal  
Designation: JS/AS Joint Secretary (eHealth)  
Email-id: alav@ias.nic.in  
Contact No: 2306 1195

For Uploading on Website

Level 1:

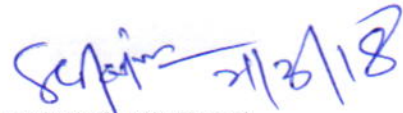
Level 2:

Level 3:

Level 4:

Uploaded on:

Uploaded by:

  
(Signature of Web Information Manager)

(लव अग्रवाल)  
(LAV AGARWAL)  
संयुक्त सचिव/Joint Secretary  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
Ministry of Health & F.W.  
भारत सरकार/Govt. of India  
नई दिल्ली/New Delhi



F.No Z-18015/23/2017-eGov  
Government of India  
Ministry of Health & Family Welfare  
(eHealth Section)

\*\*\*

Dated the 21<sup>st</sup> March, 2018

NOTICE

**Subject:** Placing the draft of "Digital Information Security in Healthcare, Act (DISHA)" in public domain for comments/views-reg.

MoHFW plans to set up a nodal body in form of "National Digital Health Authority" through an Act of parliament as a statutory body for promotion/ adoption of e-Health standards, to enforce privacy & security measures for electronic health data, and to regulate storage & exchange of Electronic Health Records.

2. The purpose of the act is to provide for electronic health data privacy, confidentiality, security and standardization and provide for establishment of National Digital Health Authority and Health Information Exchanges and such other matters related and incidental thereto.

3. The comments/views on the draft of the act may be forwarded to Director (eHealth), Ministry of Health and Family Welfare, Room No 211-D, Nirman Bhawan, New Delhi-110108 or emailed at **egov-mohfw@nic.in** on or before 21<sup>st</sup> April, 2018.

*The Hindi Version will follow soon.*

  
(S.C. Rajeev)

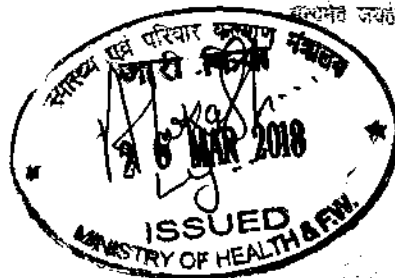
Director(eHealth)  
Phn No. 23062205



Joint Secretary

Tel : 011-23001195  
 1/Fax : 011-23001842  
 E-mail : jay@ias.in

Dear Madam,



D.O. No. Z-18015/23/2017-eGov  
 Dated: 22<sup>nd</sup> March, 2018

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders.

Salient features of draft Act include:

- i. Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to)
- ii. Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- iii. Providing for establishment of Digital Health Information Exchanges; and
- iv. Framework to provide for civil and criminal remedies for data breach.

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act for seeking your comments and suggestion on the draft act before putting this up in public domain for feedback.

With Regards,

Yours sincerely,

*[Signature]*

[Lav Agarwal]

Mrs. Veenu Gupta  
 Principal Secretary (Health & FW),  
 Department of Health & Family Welfare,  
 Government of Rajasthan,  
 Room No. 5208, Govt. Secretariat,  
 main building,  
 Jaipur-302005

+ All Pr. Secy (H) all State.  
 All JSs MoHFW

67C

10/03/2018  
 22/3

24.3.18

Shri Sudhir Kumar	JS	<i>Rant 27/3</i>
Preeti Pant	JS	<i>Pant 27/3</i>
Shri Sunil Sharma	JS	<i>Sh 27/3</i>
Shri Lav Agarwal	JS	
Shri Sudhansh Pant	JS	<i>Sh 27/3</i>
Shri Arun Singhal	JS	
Ms. Preeti Nath	EA	
VANDANA JAIN	JS	
Ms. Gayatri Mishra	JS	<i>Sh 27/3</i>
Ms. Vandana Gurnani	JS	<i>Sh 27/3</i>
MANOHAR AGNANI	JS	<i>Sh 27/3</i>

*27/3*  
*27/3/18*

*SS & FA — Sh  
27/3*

*27/3*

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
1	<a href="#">IHMIR</a>	Clause 1(1) - DISHA Clause 4 - NeHA Clause 7 - SeHA	While the forwarding letter signed by you talks of setting up a nodal body in form of "National Digital Health Authority", as envisaged in the National Health Policy 2017 (Clause 23), the accompanying draft bill talks of only the National and State eHealth authorities (NeHA/SeHA). <b>This discrepancy needs to be reconciled</b> , as per decisions taken in the multiple meetings held for stakeholder consultations and also in the meetings for drafting the Bill for DISHA.	DISHA is defined in Clause 1 (1)	Draft Act proposes to establish NeHA at the Centre and SeHA at the State.  need to review clause 21(c)

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
2	<a href="#">BMJ</a>	NA	<p>Greetings from British Medical Journal (BMJ) Publishing Group.</p> <p>With ref to your notice dated 21st Mar 2018 on the above stated subject, here I would wish to provide some information which you may find useful.</p> <p>In UK, there is a lot of regulation. This website is the main source of relevant standards and guidelines in the UK.  <a href="http://content.digital.nhs.uk/standards">http://content.digital.nhs.uk/standards</a></p> <p>Of most relevance is this content  Clinical Record Standards / Clinical Safety / Information Governance / Information Standards / HSCIC Data quality standards  I would recommend that you have a look at this in the first instance.</p> <p>Just to say that BMJ Best Practice (<a href="http://www.bestpractice.bmj.com">www.bestpractice.bmj.com</a>), a clinical decision support services (CDSS) tool aspires to operate to the highest standards in clinical decision support - especially with regard to patient safety, user and patient consent and confidentiality, and in clinical knowledge and evidence-based medicine.</p> <p>I hope this is helpful and happy to support further if need be.</p>	Suggestion provided with reference to international standards and guidelines on Healthcare	This is an Act and necessary guideline may be developed by the Authority

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
3	<a href="#">LHPL</a>	NA	<p>This e data is <b>very complex</b> for india at this stage. <b>It should be started only as a pilot project in few hospitals in different level cites of India.</b></p> <p>This provision will increase the <b>cost of treatment</b> .</p> <p>The e data can be easily hacked and also can lead to breech in <b>privacy of a patient</b></p> <p>Please consider before switching to e data</p>	Suggestion provided for rollout restricted to few health facilities initially considering complexity, security involved in larger scale	This is an act detailed guidelines for roll-out would be developed by the authority.

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
4	Dr. Prof Khandelwal	NA	I agree with the draft for DISHA. It is comprehensive.	NA	-

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
5	<a href="#">HCG</a>	NA	<p>Overall objective of the Digital Information Security in Healthcare should be integration &amp; successful implementation of eHR for population Health Surveillance System &amp; modernisation of the Information Technology infrastructure for health system for collecting, compiling &amp; analysing information of individuals from birth to death data from clinical aspect. Purpose of <b>DISHA ACT should support implementation of eHR for population Health surveillance</b> is to create and upgrade the content &amp; accessibility of basic public services in health care system to elaborate several new e – health services. Digital Information Security in Healthcare Act should develop standard and incorporate same, based on the following -</p> <p>STANDARDS/ DATA QUALITY/ DATA STRUCTURE &amp; SYSTEM DESIGN/ CONFIDENTIALITY/ SELECTION OF POPULATION HEALTH INDICATORS/ SELECTION BIAS &amp; NORMALISATION OF OUTPUT/ DUPLICATE RECORDS/ INCLUSION &amp; EXCLUSION CRITERIA/ INNOVATIVE ELEMENTS &amp; NOVEL APPROACHES TO IMPLEMENTATION</p>	Suggestion provided for Act to support implementation of Population Health Surveillance and strengthen healthcare services, develop standard considering various aspects of Health information system	May be discussed



S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
6	<a href="#">Kaushik Kanti Bhattacharya</a>	NA	<p>I've the following comments after reading the document:</p> <p>1. There is no explicit clauses on peer-to-peer health information exchange between clinical establishments. Is there any standard data exchange protocol between peer entities?</p> <p>2. If a clinical establishment doesn't have information system to store digital data, will they be out of purview of this law? Is there any mandate to generate digital health records for patient encounters? Or is it optional?</p> <p>3. There is no explicit clauses pertaining to vendors/3rd parties dealing with patient health data. I mean companies providing hosted applications for patient care (EHR, LIS, Online pharmacy etc.).</p>	<p>1. Provision in Clause 34. Sub-section(2) Access to digital Helth data. However EHR notified interoperability notified standards are not provided in the draft Act</p> <p>2. No provision in draft Act explicitly.</p> <p>3. Provision in Clause 32.<i>Storing of digital health data - Sub-section 1</i></p>	<p>Standards would be defined by the Authority, paper records are not part of the act as of now and are governed by Medical Council Code of Ethics.</p>

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
7	<a href="#">Dr. Vipul Kumar</a>	NA	<p>Although it is necessary to have DISHA, its <b>scope should be wider</b>. Insurance companies, Pharmaceutical companies (especially costly antibiotic and anticancer drugs), Multicity <b>Pathological laboratories</b> ( like SRL diagnostic, Immuno doagnostic, Dr. Lal's Pathology etc) and Large Corporate Hospitals (Apollo, Fortis, Wockhardt etc) may try to access patient's data for <b>digital marketing</b> and for other benefits. special consideration should be given to this aspect , with stringent penalties.</p> <p>Secondly, DISHA is just a single limb of the whole body of data. In fact , the law should be more comprehensive . A single comprehensive law is required which will prevent misuse of all data in Digital Form which is usually available with <b>Educational Institutions, Insurance companies, Mobile Phone companies, Employers in Business, Online Marketing companies</b>, Income tax Department, AADHAAR, Local Municipal Bodies, Driving Licence, Passport, Bank Account, Demat Account etc. All this data needs to be protected from poachers.</p>	<p>Suggestion to protect health data by including various stakeholders in healthcare under of Offences and Penalties section of DISHA Act including Insurance, Phamaceutical, Diagnostics, educational, Govt dept.</p> <p>Protection of Digital Health data from Insurance and Pharmaceutical entities provided in CLAUSE 29 (5) of the Draft Act.</p>	<p>The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.</p>

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remarks	Remarks
8	<a href="#">Manohar Mungekar</a>	NA	<p><b>Suggestion for DISHA</b></p> <p>1) Data collected by health sector should not identify the patient, and the privacy and confidentiality of data must be protected.</p> <p>2) An important parameter in e-Health information and records management is custody, the new law must address this as who are responsible for archiving &amp; or the <b>custody of e-records and information in the health sector.</b></p> <p>3) The law must also specify on how interoperability will be achieved, either by the use of open systems or any other means.</p> <p>4) For data storage appropriate standards must be applied as how the data is maintained.</p> <p>5) Medical /Health data must not be used for other purposes, other than specified except unless consented or authorised by law.</p> <p>6) The use and purpose of data collected must be defined and stated clearly.</p>	<p>Point 1: Provision in CLAUSE 29 <i>Purpose of collection, storage, transmission and use of digital health data</i> , 30 <i>Collection of health data</i> of the Draft Act.</p> <p>Point 2: Provision in Clause 30 and specifically in Subsection (4) and Clause 32 <i>Storing of digital Health data</i></p> <p>Point 3&amp;4: EHR interoperability notified standards are not provided in the Draft Act. Shall be in purview of the</p> <p>Point 5&amp;6: Provision in Clause 29 and specifically in Sub section (3)</p>	Custodian may be defined in the Act

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
9	<a href="#">InnovatioCuris</a>	Caluse 3 (i) e	<p>a. Possible Typo: In the section (3), clause (i), there is a line, "but does that include the clinical establishments owned, controlled or managed by the Armed Forces. Explanation: For the purpose of this clause, "Armed Forces" means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)".</p> <p>I think the language used probably means an exclusion, We wonder if it should be " but does not include the clinical establishments owned, controlled or managed by the Armed Forces. Explanation: For the purpose of this clause, "Armed Forces" means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)"</p>	Languaged used in Clause 3 (i) (e) may be reviewed	May be discussed
		Clause 33 & Clause 32	<p>b. Standards should not be optional but mandatory, when it comes to security: Most hospitals do not have encryption for storing records and real time backup. We have interacted with some of the leading hospitals in the country and their vendors who implement EHRs and they have confirmed the same.</p> <p>Which makes the data owners vulnerable at the time of breach and hospitals are at a stand still because of the lack of backup and patients vulnerable because of the data being in plain text.</p> <p>In clause 33, the act talks about encryption during transmission. Maybe, you can consider the same level of security, while storage by making it explicit in clause 32.</p> <p>I have written a paper, which talks about broader security risks and is available here: <a href="http://innovatiocuris.com/cyber-security-threats/">http://innovatiocuris.com/cyber-security-threats/</a></p>	<p>Encryption for storage of digital health data</p> <p>Point to be examined considering the implementation challenges and complexity involved</p>	May be discussed

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		-	<p>c. Integrity of data, going beyond the breach: We think the biggest threat we face in today's time is that of not knowing a breach has happened in terms of access to systems with out knowledge and authorisation. If the records are tempered with and the detection happens 6 months down the line. How do we know that the data values are same?</p> <p>In the stuxnet attack , the main reason of success for the malicious program was by learning the normal values of the healthy system and showing them to the experts, while at the same time damaging the nuclear plant by over spinning the centrifuges.</p> <p>After the first cyber attack of the world, Estonia developed such technology to take care of data integrity. As they fear that the data integrity would be compromised and they would not even come to know. Hence, they use block chain technology for that. <a href="https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/">https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/</a> . We suggest for important databases integrity preservation is very important in connected world. Estonians go to an extent by printing their database hash monthly in the financial times.</p> <p>The word integrity is used in the act document twice for chairperson to head the authority, maybe we could also consider the same for the digital health data.</p> <p>We strongly believe that we should consider the measures that establishments should take for making sure that the data they have stored is having its integrity. Else, in the medical domain, data that has been manipulated could be life threatening!</p>	May be kept in the purview of NeHA committee proposed in the draft Act, considering implementation norms and envisaged benefits	May be discussed
		Clause 34	<p>d. Empowering the citizen: In the clause 34, the act talks about access to digital health data.</p> <p>In Estonia for example, the citizens using their national id can see logs of, 'who has accessed their data'. This is very empowering context, no other country in the world provides such transparency and empowerment to citizens.</p> <p>In the almost Orwellian world, people question who will watch the watcher (big brother). It becomes very important to consider steps such as making it important to create access logs and if possible provide citizens (owners) the access, that who has viewed their data! Such a linked portal with an identity like Aadhar might even empower citizens to rectify the details as mentioned in the act in the clause 36.</p>	<p>Provision in Clause 34 sub-section (5).</p> <p>May be kept in the purview of NeHA committee proposed in the draft Act, considering implementation norms and envisaged benefits</p>	May be discussed

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		Clause 35	<p>In case of breach: As per clause 35, within the three days of breach the clinical establishment should inform the data owner impacted. Statistics suggest, it takes 6 month to detect a breach. <b>So, what happens to those breaches which are detected later than 3 days?</b></p> <p>In the cyber security industry they say, there are two kind of organisations. One who know that they have have been hacked and one who does not.</p> <p>Last but not the least. I believe that this act can generate many new jobs and opportunities, if India takes the lead and sets an example for the world! There are many parallels of this act and what is happening in EU with GDPR .</p> <p>We believe as a next step we should have a roundtable discussion on "How DISHA Act can create more jobs and opportunities" and invite the cyber security companies and clinical establishments to brainstorm the opportunities and challenges.</p>	Caluse 35 sub-section (5) may be discussed	<p>May be discussed.</p> <p>Breach identified later may be addressed in the act or should be defined by the auhtority.</p>

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
10	<a href="#">Kalpataru MC Hospital</a>	NA	1. Software vendors Most of the doctors are software illiterate. Sql databases and data sanitisation is well left to software people. Make them liable to build up security along with the software. Any data breach needs lapses from the developer side too. We as customers face a lot of resistance from their side as they have absolutely no accountability.	Provision in Caluse 31 Ownership of digital health data	Implementation issue
		NA	2. Cloud Most of the vendors push data that is served from the internet as a solution. While this is great it is important to note that health data saved on the cloud is at the mercy of the paid subscriptions and internet access. Any off site data security should be addressed.	Provision in Chapter IV Data Ownership, Security and Standardisation	Implementation issue
		NA	3. Framework for data storage and access/ usage of established standards for data storage One word HIPPA	Sugestion provided for data storage standards	Implementation issue
		NA	4. Insurance companies will be lefy out of this data. A look at the usa mess is enough.	Provision in Caluse 29/5	Anyone having patient data in electronic form is covered under the act.
		NA	5. Training for doctors Very essential as most of them find it as an added step and a hurdle.	Provision in Clause 35 sub section (4) " <i>Duty to maintain privacy and confidentiality of digital health data</i> "	Implementation issue

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
11	<a href="#">Vietnam Embassy</a>	NA	<p>With National Electronic Health Authority, the bill should include provisions allowing NEHA to conduct multilateral, bilateral and multilateral co-operation activities in order to further improve India's system of eHealth. This is perfectly appropriate because India now has good diplomatic relations with ASEAN countries, the formation of a unified standard of e-health records or a unified standards of medicinal testing information system or a unified health information exchanges is quite important, this will make it easier for India to connect with ASEAN, in line with the Digital Connectivity Policy pursued by Modi's government, and in line with current practice in India, because your country has many successes in terms of medical tourism, which can attract large numbers of foreign visitors to India for medical treatment.</p> <p><b>Vietnam and India have also signed MOUs on health cooperation, signed in September 2016, but the two countries do not currently have many bilateral health cooperation.</b> Therefore, we hope that digital healthcare sector in the future will be an important pillar in the healthcare cooperation between the two countries' Health Ministry</p>	Anticipation of active bilateral, multilateral Cooperation in Health through MoU signed between Vietnam and India in Sep 2016, from the provisions proposed in the Draft Act.	May refer to powers of authority, if required a sentence may be added.



## 909695/2018/E-GOVERNANCE

S.No	Organisation	Draft Act Clause No	Comment	Finding	Remarks
12	<a href="#">Parthasarathy Sridharan</a>	Caluse 37 & 38	<p>I am S.Parthasarathy, a chartered accountant by profession. I have given two suggestion to the draft DISHA act so as to increase its deterrence effect.</p> <p>Stringent penalty for breaching digital health data for commercial considerations. Clause to be added to deter breach of digital health data.</p> <p>Sections 37 and 38 talks about breach and serious breach of data respectively. Section 37 awards compensation while section 38 penalizes perpetrator with compensation and imprisonment &amp;/Or fine which shall not be less than Rs.5Lakhs.</p> <p><b>The penalty clause needs to consider the commercial context of the breach of data.</b></p>	Suggestion provided for Chapter V Offences and Penalties	May be taken up for discussion.
		NA	<p>Generally, with data being the 21st century oil driving commercial considerations and targeted advertisements, various commercial entities may benefit tremendously disproportionate to the fine amount from breaching the data. Hence, the penalty clause should include the concept of</p> <ul style="list-style-type: none"> <li>· disgorgement of profit earned due to the breach of data or</li> <li>· fine amount needs to be in multiples of illegal profit (say 2x or 3x) earned in lines similar to security law.</li> </ul> <p>This ensures sufficient deterrence for commercial entities.</p> <p>Include DNA data in the definition of Digital health data explicitly</p> <p>With technological advancements, genome sequencing is altering the diagnostic landscape of the world. With increasing competition and technological advancements, price barrier may decrease and substantial population will be driven towards DNA sequencing considering the immense personalized medical treatment possible.</p> <p><b>Hence, with the current section 3(e), digital health data fails to unambiguously recognize DNA data</b></p>	Suggestion for Chapter V Offences and Penalties	May be taken up for discussion.

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
13	<a href="#">Dr. Abhijit Poddar</a>	NA	1. The entire law has not specified any regulation on Internet traffics that could exchange the digital data. We are approaching to a time where artificial intelligence, machine learning shall dominate the cloud operations in digital space and may use it to challenge national security. For such, these new developments should be considered in this policy so as to protect privacy as well as national security. <b>An overlap or connection with existing digital data security policies should be provided.</b>	Concern expressed with data security and any overlap with existing digital security policy	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.
		NA	2. In general, security concerns arise from both intentional and unintentional approaches of data handling. <b>DISHA have covered many of intentional breach scenarios, but no provisions and the guidance are available on unintentional cases that may arises from poor data storing system, use of virus infected and backdated software and systems, inattentive/ poorly attentive database management systems etc.</b> Although, in Sec 22, clause 1(b) both scenarios have been covered by 'To ensure data protection and prevent breach or theft of digital health data, establish data security measures for all stages of generation, collection, storage and transmission of digital health data, which shall at the minimum include access controls, encrypting and audit trails;'	Concerns expressed on "No provisions for breach of digital health data unitentionally". May be discussed.	May be taken up for discussion
		1. Short title, extent	Clause reads 'It extends to whole of India except the State of Jammu and Kashmir.' <b>In digital space, geographic boundary has limited rationale.</b> A person/ group sitting in J&K may take control of digital data of other parts of India as well as globe. In view, <b>DISHA should cover whole of India including J&amp;K.</b>	This means only of the patient data pertaining to J&K and not to those who commit crime based in J&K	No Action required
		3. Definition (e) Digital Health data	Clause reads 'means an electronic record of health related information about an individual'. In addition to individual centric information, <b>the scope of health data may cover community specific health related information; entire database stored in particular healthcare system.</b> In contrast to individual data, malicious interests are more directed towards acquiring community specific information so as to identify vulnerability and prepare strategies to introduce threat to our nation. This is particularly true for involvement of non state actors to introduce biological weapons as part of bio-terrorism.	Clause 3 (e) 'Digital Health Data'	Covered under the Act

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		3. Definition (f) entity	An association of persons or a body of individuals, whether incorporated or not, in India or outside India. 1. The section covering person outside India may be emphasized. For such relevant experts of National Security Act may be adopted and is mentioned herewith: "foreigner" has the same meaning as the Foreigners Act, 1946 (31 of 1946); "person" includes a foreigner; 2. Further, even it covers person/ organization abroad, how to locate them as digital data being a non-physical entity, may be theft from outside over the internet. In view, in extent, the law may also cover all INTERNET traffics that circulate, come and go from India.	Reference to 'National Security Act' provided for consideration under Caluse 3 (e) Entity	May be taken up for discussion
		3. Definition (n) Data Security'	Clause reads 'to protect the privacy of health information' In addition to privacy protection, data security shall also aim towards protection of health data from the inadvertent, inappropriate, or intentional malicious or malevolent use with an aim to design biological threat agents to introduce bio-terrorism.	Protection of health information privacy from unitentional disclosure	May be taken up for discussion
		3. Definition (o) 'Sensitive health-related information	Sensitive health related information should be a part of digital health data. Further it contains few terminologies that are not covered in digital health data although mention here. As part of sensitive information, <b>all communicable disease burdens</b> should also be considered. The word harm needs to be defined.	Suggestion for sensitive health-related information to cover all communicable disease burden	May be taken up for discussion
		5. Composition of National Electronic Health Authority of India	1. With such top notch bureaucratic composition, who will do the ground research? How the State committee will be connected with the apex body? 2. Further as data breach could encompass people/ organizations outside India, how this committee shall respond to such threat in absence of participation of MEA? 3. Health data could be used as a tool to design and deliver bio-weapons and obviously a threat to national security. In this connection, without NIA on-board, which is empowered to act under 2005 weapons of mass destruction act, enactment of national security in part of health security shall not be possible. In this matter, only DBT can define and grade the data which may be used for inappropriate purposes to design bioweapons. Hence, inter-ministerial involvement with these relevant ministries should be considered.	Suggestion for Composition of NEHA. Inter-ministiral involvement on national security related issues. May be discussed	May be taken up for discussion
		8. Composition of State Electronic Health Authorities	The participation of workforces who are actually in ground is missing in the entire composition. State should identify all healthcare systems and may appoint the person appropriate who can connect, train and monitor health data being generated in each state.	Suggestion for composition of SEHA	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		22. Powers and functions of National Electronic Health Authority of India	Ensuring digital health security is not a static process rather shall require dynamic improvements as and when required. In this direction, it may cover : 1. "To train and foster adequate manpower to deal with future challenges in digital health security." 2. 'To grade the digital health security data pertaining to national security and develop regulations of those accordingly.'	May be discussed and considered	May be taken up for discussion
		38. Serious breach of digital health data	1. Serious data breach can also occur by a group/ organization either operating at States or abroad, so the scope and related penal provisions should be justified accordingly. 2. The scope may also include 'theft of highly sensitive data that may compromise national security'. 1. Serious data breach can also occur by a group/ organization either operating at States or abroad, so the scope and related penal provisions should be justified accordingly. 2. The scope may also include 'theft of highly sensitive data that may compromise national security'.	May be discussed and considered	May be taken up for discussion
		38. Serious breach of digital health data:	Clause reads " A breach of digital health data occurs where a person failed to secure the data". I disagree with point c. In spite of his/her best efforts, digital health data may be stolen. For e.g., every now and then hackers attempt to take control of govt sites and sometimes succeed. In such case, the person shall not be liable to punishment rather we should try to provide more emphasis on Internet security.	Point 38 (c) may be discussed	May be taken up for discussion
		42. Data theft	The penal provisions for data theft have been mentioned in earlier sections.		

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
14	<a href="#">USISPF</a>	NA	<p>Greetings from U.S. India Strategic Partnership Forum, a non-profit organization focused on strengthening business relations between the U.S. and India, and enhancing the U.S.-India strategic relationship. We are committed to creating the most powerful strategic partnership between the two countries. Promoting bilateral trade is an important part of USISPF's work, but USISPF's mission reaches far beyond this. We believe it is about business and government coming together in new ways to create meaningful opportunities that have the power to change the lives of citizens. USISPF is headquartered in Washington DC, with offices in New York, Silicon Valley, Delhi and Mumbai.</p> <p>USISPF appreciates the efforts of the Ministry of Health and Family Welfare towards setting up a nodal agency in the form of "National Digital Health Authority" for promotion/ adoption of e-Health standards.</p> <p>We are in the process of collating feedback and inputs from our member companies on the draft order that has been circulated on 21st March. Since this has deep implications for both the Technology and Health Sector, <b>we would request you to kindly extend the timeline for feedback and inputs to at least 15th May.</b> The extension would allow us sufficient time to get inputs from all stakeholders across the board.</p> <p>I shall be in touch with your office to follow up on this request.</p> <p>Once again, we thank you for your support and look forward to your favourable consideration of our request.</p>	Request for extension of time for submission of comments	No action

S.No	Organisation / Institution	Draft Act Clause No	Comment	Remarks	Remarks
15	<a href="#">Adv. Surbhi Guptha</a>	Clause 3 (a) (d)	<p>Pursuant to my telephonic discussions with the Section Officer Ms. Amita Ved, I have been asked to write on this mail id for seeking a clarification regarding the DISHA Act. As you would already be aware the Ministry of Health and Family Welfare, Government of India has introduced the draft of the Digital Information Security in Healthcare Act (the "Act") for public consultation. We seek to give our views / recommendations on the same.</p> <p>In this regard, we understand that the Act differentiates between Anonymization and De-identification of digital health data. As defined in Section 3 (a) of the Act, the term 'Anonymization' means the process of permanently deleting all personally identifiable information from an individual's digital health data. On the other hand, as defined in Section 3 (d) of the Act 'De-identification' means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.</p> <p>Section 29 (5) of the Act provides that digital health data, whether identifiable or anonymized, is not permitted to be accessed, used or disclosed to any person for a commercial purpose and in no circumstances can it be accessed or utilised by insurance companies, employers, human resource consultants and pharmaceutical companies.</p> <p><b>Our query is whether there is any restriction on use of de-identifiable digital health data as well.</b> Kindly respond at the earliest and oblige as we wish to submit our recommendations on the draft Act shortly.</p>	May be clarified under Clause 29. Purpose of collection, storage, transmission and use of the digital health data	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remarks	Finding/Remarks
16	<a href="#">Nilotpal Chakravarti</a>		<p>Greetings from the Internet and Mobile Association of India (IAMAI)</p> <p>This is with regard to the draft of "Digital information Security in Healthcare, act (DISHA)" in public domain for comments/views.</p> <p>It gives me pleasure to inform you that IMAI has set up a result oriented Committee on HealthTech. The mandate of the committee is to fast-track adoption of technology in the healthcare space and how technology can redefine the availability of affordable healthcare for all concerned. Some of the members of the committee include Netmeds, Practo, IBM, Credihealth, to name a few.</p> <p>As an association, IMAI represents the Digital Ecosystem in India with over 300 members [Indian and MNC] representing the entire gamut of digital services in India. On behalf of the Committee on HealthTech, I would request you to please grant an extension of the said deadlines, as members are still studying the draft and are in the process of sharing their feedback with us. We on behalf of the industry are keen to share our feedback/suggestions, <b>and hence an extension for 15 days would be highly appreciated.</b></p> <p>Look forward to your positive intervention.</p>	Extension Requested for submission of comments	No action

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
17	<a href="#">IMA</a>	28 (8)(a)	28(8)(a) The right to rectify without delay, from the respective clinical establishment or health information exchange or entity, any inaccurate or incomplete digital health data, in the prescribed form as may be notified by the National Electronic Health Authority;  <b>Comment: Patient should notify the CE, with copy to HIE, regarding inaccuracies or incompleteness of the health data; which CE should rectify within stipulated time. IF CE fails to rectify, then HIE should rectify the data.</b>	Suggestion provided may be taken up for discussion and placed with NeHA	May be taken up for discussion
		28 (8)(b)	28(8) (b) The right to require their explicit prior permission for each instance of transmission or use of their digital health data in an identifiable form, through such means as may be prescribed by the Central Government;  <b>Comment Is the consent to be taken once at the time of registration, or at the time of each encounter? Whether the consent should be on paper, signed by patient and his relative or electronic? Should the consent also include permission to HIE to allow access to information by another CE?</b>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		28 (8)(c)	28(8)(c) The right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 34 of the Act;  <b>Comment: Whether the HIE will send notification on patients mobile / email to patients email ID?</b>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		28 (8)(d)	28(8)(d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;  <b>Comment: Whether the CE has to confirm identity and relationship of the family members as per definition in 3(1)(m) before sharing the digital health data? Why this responsibility should not be entrusted to HIE.</b>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		29(2)	29(2) Digital health data may be generated, collected, and stored by any other entity for the purposes mentioned in clauses (a) to (c ) of Sub-Section (1)  <b>Comment : Whether such entity will be pre-registered under DISHA act or whether software used by the entity will have to get license/certificate from recognized agency / HIE to which it transmits?</b>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority



## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		29(5) Para 3	<p>29(5) Para 3: Provided that for the purpose of processing of insurance claims, the insurance company shall seek consent from the owner to seek access his or her digital health data from the clinical establishment to which the claim relates</p> <p><b>Comment: This clause will create various administrative issues. The insurance company should access data from HIE directly with consent of the patient. What if patient does not give consent to CE but gives consent to insurance company? In that case, CE cannot transmit data to the insurance company or to the HIE.</b></p>	May be discussed	May be taken up for discussion
		30(5)and(6)	<p>30(5)and(6) Provided that.. shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.</p> <p><b>Comment: What happens to the data which has been transmitted to HIE by the CE. Whether it is responsibility of CE to delete the data from HIE or whether CE should forward the request to HIE which will do the needful under advice to CE?</b></p>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		33(2)	<p>33(2) A clinical establishment may transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the clinical establishment.</p> <p><b>Comment: What happens if the encryption protocol used by CE is different from one used by HIE or one used by other CE which accesses the data on a later date.</b></p>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		33(3)	<p>33(3) The digital health data shall be transmitted by a clinical establishment or entity or health information exchange only upon the consent of the owner,</p> <p><b>Comment: Is the consent to be taken at the time of every encounter or one time at the time of registration with CE?.</b></p>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		33(4)	33(4) A health information exchange shall maintain a register in such form and manner as may be prescribed by the Central Government, containing all details of the transmission of the digital health data between a clinical establishment and health information exchange, and between health information exchanges inter se. <b>Comment: Between HIE and CE should be added to above list.</b>	Formulation of standards, operational guidelines and protocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		34(4)	34(4) In case where access to digital health data is necessary for the purpose of investigation into cognizable offences, or for administration of justice, such access may be granted to an investigating authority only with the order of the competent court; <b>Comment: What happens if person who is being investigated for cognizable offense withdraws the consent given to the CE? Also if the HIE provides data to the investigating authority before CE deletes the data from the HIE?</b>	May be discussed	May be taken up for discussion
		34(5)	34(5) The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India. <b>Comment: Whether this should remain "access only" is important issue. Patient should be able to add/edit personal health record which will help to facilitate tracking of various parameters such as blood sugar, pulmonary function test, exercise record etc which are important in monitoring chronic diseases. Data generated by CE should be only accessible to patient and data generated by patient should be only accessible to CE</b>	Scope of creation, access, modification of digital health data by any entity be placed for discussion with NeHA	May be taken up for discussion
		34(6)	34(6) In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified; <b>Comment: Certain should be replaced with ALL. Will the CE get identity of the patient in emergency based on his thumb impression? This is essential for management of unidentified victim of accident who has to be treated and stabilized by CE as per Supreme Court Ruling. It becomes difficult to continue treatment after initial stabilization, and if the patient is transferred to government institution, usually the patient is lost to follow up. (Charges for treatment given cannot be recovered from anyone.)</b>	Suggestion provided may be taken up for discussion	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		34(8)	<p>34(8) Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner.</p> <p><b>Does this mean that at the time of consent the CE should ask the patient to give list of legal heirs to whom access should be given and who are barred expressly? Such consent will have to have a statement as under “In case of my death...”, or whether the CE should ask for copy of will/ affidavit?</b></p>	Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		34(9)	<p>register in a digital form to record the purposes and usage of digital health data accessed within the meaning of this Section, in such form and manner, as may be specified by the National Electronic Health Authority.</p> <p><b>Comment: Whether such register should be maintained in electronic format or it is required to be maintained in physical format. ? If HIE can provide electronic register of access of data of any patient by any stakeholder, it will avoid duplication of effort. CE should record data generated from patient and transmit the same to HIE. Ambiguity is likely to be generated if register is maintained by both HIE and CE. As another CE can accesses the data from HIE, it will be better if HIE records the access from CE rather than CE creating another register.</b></p>	Suggestion provided may be taken up with NeHA and as per Clause 22	May be taken up for discussion
		35(5)	<p>35(5) A clinical establishment, or a health information exchange, shall provide notice immediately, and in all circumstances not later than three working days to the owner, in such manner as may be prescribed under this Act, in case of any breach or serious breach of such digital health data.</p> <p><b>Comment: Whether this duration of 3 days is from date of breach or from date of getting knowledge of the breach?</b></p>	May be discussed	May be taken up for discussion
		36 (2)	<p>36 (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.</p> <p><b>Comment: How can HIE rectify any data without intimation to the CE which created the data. e.g. information regarding allergy to a drug was not given by patient to the CE. Later he asks the HIE to make correction without knowledge of the CE. This will lead to legal complications and unrest amongst CEs.</b></p>	Implementation Specific Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority
		37(1)(d)	<p>37(1)(d) Any person damages, destroys, deletes, affects injuriously by any means or tampers with any digital health data</p> <p><b>Comment: What happens if the patient removes the consent with request to delete data stored by CE or transmitted to the HIE?</b></p>	Implementation specific Formulation of standards, operational guidelines and potocols shall be under purview of NeHA as per Clause 22	Standards would be defined by the Authority

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		37(2)	37(2) Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place.  <b>Comment: How can it be proved that the breach happened at the HIE level and not at CE level? The breach of data is not likely to be of one patient. It will be of all patients treated by one CE, or transmitted to HIE by all CEs.</b>	May be discussed	May be taken up for discussion
		38 (1) (c)	38 (1) (c) A breach of digital health data occurs where a person failed to secure the data as per the standards prescribed by the Act or any rules there under; or  <b>Comment: What are said standards? They have not been clarified in this act. The Electronic Health Record standards rely heavily on Aadhaar number, which has been mentioned in schedule I. What is current status of Aadhaar Number w.r.t. confidentiality of information? Has Supreme Court approved use of Aadhaar for HIE?</b>	Formulation of standards, operational guidelines and protocols shall be under purview of NeHA as per Clause 22	May be taken up for discussion
		38(2)	imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.  <b>This provision will discourage all CEs from digitization of health data. Instead of taking consent for collection of digital health data and transmission to HIE, they will take consent for not to digitize data; or to digitize data but not to transmit it to HIE. If the patient refuses consent, NEHA or any other act cannot force CE to collect and transfer health data. Purpose of this act, IHIP and NEHA will be defeated as no data will be available for public health decisions. At least in first few years of NEHA, such legal provision should be avoided.</b>	May be discussed	May be taken up for discussion
		40(1) (2) (3)	40(1) (2) (3) Any Person  <b>Comment: Person: should it be entity (whether EDP manager of hospital or Hospital as organization)</b>	May be considered in Caluse 40 (1)(2)(3)	May be taken up for discussion
		43(1)	43(1) No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made there under, save on complaint made by the Central Government, State Government, the National Electronic Health Authority of India, State Electronic Health Authority, or a person affected.  <b>Comment: What if CE has any complaint about HIE / Owner of the data? There is no provision to grant any remedy whatsoever to the generator of digital health data, who has nothing to gain from such digitization? Why would CEs assist MOH&amp;FW by generating and transmitting digital health data, given the unfavorable circumstances created for CE by virtue of this act?</b>	May be discussed	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		45(5)	45(5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Electronic Health Authority under section 40 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.  <b>Comment: This appeal is after getting the order. What about complaint against HIE/Owner of data?</b>	May be discussed	May be taken up for discussion
		46(4)	46(4) Notwithstanding anything stated in either sub-section (3) or (4) above, the Adjudicating Authority may by order extend the time period, and entertain the complaint made after lapse of time;  <b>Comment: it should be 2 or 3 instead of 3 or 4</b>	May be considered in Clause 46 (4)	May be taken up for discussion
		46(5)	46(5) Any person or entity aggrieved by the order, direction or penalties imposed by the State Electronic Health Authority under section 40 of this act, may prefer an appeal to the State Adjudicating Authority within a period of forty-five days from the date on which a copy of the order is received.  <b>Comment: This appeal is after getting the order. What about complaint against HIE/Owner of data?</b>	Clarifications requested on offences and penalties	May be taken up for discussion
		Schedule I: (xiii)	Schedule I: (xiii) Medical records and history;  <b>Comment: Should not be included in personally identifiable information as it is required for public health purpose.</b>	May be discussed	May be taken up for discussion
		(xvi)	(xvi) Any government number, including Aadhaar  <b>Comment: Without Aadhaar linkage HIE is difficult if not impossible.</b>	Suggestion provided for Schedule 1	May be taken up for discussion
		New Issue:	New Issue: We should not disallow direct sharing of identifiable data for direct patient care between two hospitals.  Direct sharing of identifiable data should be strictly prohibited. All exchange must be via HIE.	May be discussed	May be taken up for discussion
		NA	<b>Important consideration:</b> 1. Can data generated by another CE after patient's encounter with first CE be accessed by first CE? This has medico-legal ramifications, hence should be thought carefully. 2. How does government plan to include data generated by AYUSH doctors as there are no standards specified for these specialties. 3. What is the procedure for getting the software licensed by vendors, and getting licensed software by CEs so that software glitches can be minimized and chances of misuse of information are reduced?	1. & 3 Formulation of operational guidelines and protocols shall be under purview of NeHA as per Clause 22	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		NA (Conclusion)	<p><b>In conclusion, IMA Pune primarily and strongly objects to DISHA Act for following reasons:</b></p> <p>1. Implementation of various acts for healthcare has created problems to healthcare providers and facilitated increase in corrupt practices in health departments of government. For example:</p> <ul style="list-style-type: none"> <li>a. Consumer protection act : 90% cases frivolous</li> <li>b. PCPNDT act : Harassment, no improvement in sex ratio</li> <li>c. Clinical Establishment act : Draconian provisions, Karnataka doctors went on strike</li> <li>d. National Medical Commission : IMA had to call for nationwide strike</li> <li>e. Registration with Authorities (Qualified nurses : not available, Fire NOC : corrupt practices, Building department /Taxes : irregularities at municipal corporations)</li> <li>f. Violence against healthcare professionals: implementation of act is not seen on ground.</li> <li>g. CPCB act: Sewage treatment plant for hospitals having more than 10 beds?</li> <li>h. Experience with implementation agencies is not good and harassment is likely.</li> </ul>	Comments provided on past experience with various healthcare Acts and challenges involved.	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		NA	<p>2. There is no financial support from government / Ministry of Health and Family Welfare for implementation of health information exchange.</p> <p>3. Accessibility and Equitability issues: Cost of Healthcare will increase as expenditure on the IT infrastructure and Software will have to be recovered from the patients.</p> <p>4. Doctors are not techno-savy as far as database management and health information exchange is concerned. They have to rely on staff having knowledge in information technology. Vicarious liability of any misdeed done by hospital staff is likely to bring doctors in trouble.</p> <p>5. Clinical establishments have no control on personnel in health information exchange who are more likely to leak data to those, who can leverage benefit from analysis of the data.</p> <p>6. MOH&amp;FW notification dt. 28/10/2014 asks clinical establishments to keep data in electronic format for unlimited period and hard copy for 3 years (10 years in MLC). Why both necessary?</p> <p>7. Privacy and Confidentiality: Some acts e.g. MTP act do not allow doctors to disclose information to any third party. HIE in such cases even with consent will be construed as criminal offense.</p> <p>8. Clinical establishments should not be required to provide data to patients, insurance companies, other clinical establishments and Health Information Exchange. CE should give data to patient who may transfer the data to other stakeholders including patient's relatives.</p> <p>9. Punishment provided in the act is not graded as per severity of crime. 5 year imprisonment and Rs. 5,00,000/= fine are too harsh. There should not be criminal prosecution and erring doctor should be given warnings (three times) and finally closure.</p> <p>10. Aadhaar Card is not available to each citizen and use of this number has not been authenticated by Supreme Court of India.</p>	Comments provided on Challenges and limitations envisaged in implementation of the proposed Act	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
		NA (Recommendations)	<p>Recommendations: Concept of Digital Information Security and HIE are good and essential for having health database of entire population. However population of our country is huge &amp; diverse.</p> <p>1. The act should be implemented in phased manner, initially only for exchange of information of:</p> <ul style="list-style-type: none"> <li>a. Notifiable Diseases (exemption from punishment for disclosure of information under CRPC, and Offense under IPC if not reported to appropriate authority already exists which should be strictly implemented.) This will remove necessity of consent from the patient.</li> <li>b. Pregnancy related information from diagnosis to delivery which will help to improve sex ratio.</li> </ul> <p>2. Ministry of health and family welfare should provide financial assistance for</p> <ul style="list-style-type: none"> <li>a. Training of manpower / skill development</li> <li>b. IT infrastructure / tax benefits to hospitals</li> <li>c. Internet connectivity and bandwidth utilization</li> </ul> <p>3. Review of utility of digital record systems such as MCTS, HMIS, IDSP etc and policy related statistics of implementation of these programs in various states will help framing strategies for implementation.</p>	Recommendations provided for implementation of the proposed Act	May be taken up for discussion



S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
18	<a href="#">HealthQuad</a>	Clause 38	<p>1. Section 38 talks about the serious breach of health data in which sub-section (1), clause (d) says “A serious digital health data breach shall be said to have taken place” if “Any person uses the digital health data for commercial purposes or commercial gain.”</p> <p>My comment: <b>The point is a valid point as far as individual patient data is concerned. However, the breach should not be applicable to anonymized data at the population or a cohort level.</b> This anonymized data, as highlighted, will be the very data which will help to draw population health insights, epidemiological predictions, chronic care management, personalized care pathways and artificial intelligence in healthcare. The use of the anonymized data for these purposes is already included in Section 29, clauses (d) to (h) of sub-section (1). However, commercial viability of all the data analytics and AI companies must be kept in mind to create sustainable and efficient models that will help drive India’s healthcare revolution going forward. The government could create appropriate guidelines for companies to anonymize and use healthcare data for the above purposes.</p>	Caluse 38 may be discussed in the context of anonymised data at the population or cohort level	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
19	<a href="#">CII</a>	NA	<p>We would like to congratulate the MoHFW for taking the initiative in setting up a nodal body in form of "National Digital Health Authority" through the Act of parliament as a statutory body for promotion/ adoption of e-Health standards, to enforce privacy &amp; security measures for electronic health data, and to regulate storage &amp; exchange of Electronic Health Records. We have reached out to our members and are encouraging them to deliberate on the various issues to facilitate CII compile recommendations on DISHA for submitting to your office.</p> <p>Given the complexity of the topic, especially when there are a few overlaps with the Justice Srikrishna committee white paper, Industry members are taking time to articulate their views on the various issues, and meeting the April 21st deadline for submission of response would be difficult for Industry members, and also for CII to compile.</p> <p>We believe that both DISHA and Data protection frame work will have a long term impact on the policy and legal framework of the country. It is therefore important that stakeholder are given adequate time to respond and share their suggestion.</p> <p>We are writing to you to request you to please grant an extension of six weeks and allow us time till 4th June 2018 to finalise views and responses.We look forward to your kind consideration</p>	Extension Requested for submission of comments	No action

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
20	<a href="#">Symantec</a>	NA	<p>May we bring the following points to your kind consideration:</p> <p>On 31 July 2017, the government of India had already set up a committee of experts chaired by Justice Srikrishna to enunciate the underlying principles for a comprehensive data protection framework for India. The aforesaid committee had issued a white paper on 27 November 2017 and invited comments on the same. The committee had also organized four open house discussions in different cities. It is pertinent to mention that the white paper dealt with inter alia the personal data in the context of healthcare and the medical field.</p> <p>Copy of Symantec's submission to the white paper is enclosed for your ready reference and kind perusal. As mentioned therein, we would like to underscore that the healthcare data should be treated as sensitive personal information (SPI) and therefore deserves a higher level of protection than the personally identifiable information (PII). However, to avoid likely overlap and potential inconsistency, the Government should institute a coordination mechanism to ensure consistency, compatibility and harmonization across the extant and ensuing policy and legislative developments pertaining to data protection across the respective sectors.</p> <p>Specifically, we hereby request the MoHFW to interact with the Expert Committee and other sectoral regulators to duly take into consideration the implications of the draft DISHA for the broader digital ecosystem. This will pave the way for development of a comprehensive data protection framework for India to act as the base foundation, upon which sector-specific initiatives can be built, if and when so warranted.</p> <p>Accordingly, in our humble view, it would be prudent for the MoHFW to defer further development and discourse on the draft DISHA till the outcome of the Expert Committee is available.</p> <p>We would be too happy to clarify and respond to any query that the MoHFW may have in this matter or with respect to our prior submission to the Expert Committee</p>	Reference to Justice Srikrishna Committee given for data protection framework. Suggested to ensure consistency, compatability, harmonisation across to ensure policy, legislative developments pertaining to data protection across the respective sectors	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
	<a href="#">DUA Consulting</a>	3 (1) (a)	<p>Anonymisation means the deletion of "identifiers" that could lead to the revelation of PII or the identification of the data owner, not the removal of PII itself. This makes the definition a process driven definition as opposed to a definition focused on outcomes. In cases where all PII is deleted but the owner may be identified in the course of processing, it would be difficult to fix liability or to arrive at an appropriate remedy for the same. We believe that, in order to create a transparent regulatory system with appropriate checks and balances and one which treats stakeholders equitably, it is important to reconsider this definition. Further, as has been recognized by the Sri Krishna Committee, Big Data processing and the widespread use of probabilistic reasoning therein has led to a situation where it is becoming increasingly impossible to completely and permanently anonymise data. Even data sets stripped of all usual identifiers have been used to arrive at the identity of the data owners in some academic studies.</p> <p><u>Recommendation:</u> Given the comment, and also given the fact that it is essential for a law to stand the test of time, <b>we would recommend that the definition of anonymisation as it stands be deleted from this Bill. Since the Bill already recognizes the concept of "de-identification", the same should be redrafted to impose a higher burden of compliance on part of any data controller</b> (in the present case- clinical establishments, health information exchanges etc.). This would create a limited safe harbor for such entities as well as protecting data owners from unintended consequences of Big Data processing.</p>	Recommendation provided for definition of Anonymisation. May be discussed	May be taken up for discussion
		3 (1) (c)	<p>'Consent' means expressed informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data. Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.</p> <p><u>Recommendation:</u> The definition should be redrafted in a manner that makes it clear that it is the responsibility of the service provider to ensure that the nature, purpose and consequences of processing are communicated in an understandable and accessible manner to the data owner. (may include regional language translations, verbal explanations etc)</p>	Recommendation provided for definition of "Consent"	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		3 (1) (d)	<p>'De-identification' means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.</p> <p>As in serial no 1, this definition is unduly focused upon the process of de-identification and does not give sufficient weight to the outcome sought to be achieved by such process.</p> <p><b>Given that the use of de-identification under this Bill is similar to the use of pseudonymisation envisaged under the EU GDPR, we would recommend the use of the latter term.</b></p>	Recommendation provided for definition of De-identification. May be discussed	May be taken up for discussion
		3 (1) (g)	<p>'Guardian' means a guardian recognised under any law for the time being in force. This definition is unclear. We believe that continuing with the present definition might lead to litigation in the future regarding who the appropriate person for the exercise of rights of minors under this Bill.</p> <p>Recommendation: <b>We believe that reference should be made to a single law for the purposes of determining guardianship.</b></p>	Recommendation provided for definition of guardian. May be discussed	May be taken up for discussion
		3 (1) (h)	<p>Health Information Exchanges</p> <p>(1) The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act</p> <p>(2) No entity shall function as a Health Information Exchange unless established as such by the Central Government</p> <p>While the objects of the Act clearly state the establishment of health information exchanges as being amongst them, neither the definition section nor this section define what a health information exchange is. <b>We feel it would be a major oversight to not set out the parameter for determination of what a health information exchange is in the Bill and it could, in the future lead to considerable litigation upon the scope of this Bill.</b></p> <p><u>Recommendation</u> "Health Information Exchange" should be defined. Reference may be made to USA's Federal Trade Commission's May 2014 report on Data Brokers. The said document defines data brokers as follows- "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud."</p>	Recommendation provided to include Role of Health Information Exchange. May be discussed	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		3 (1) (k)	<p>‘Personally Identifiable Information’ means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I.</p> <p>Recommendation:  <b>We would recommend the use of a definition akin to that of the European Union’s GDPR defines personal data as any information relating to an identified or identifiable natural person.</b> An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p><b>Further, we believe that the legislation should define the terms “data” and “information”. Specifically, Information’, for purpose of this bill, should cover any recorded word, act, hearsay, etc. stored in whatever form and manner. Similarly, Data should be defined in a manner as to cover any Data, written or electronic, encrypted or non encrypted, readable form or non-readable form.</b></p>	Recommendation provided for definition of Personally Identifiable information, Information, Data	May be taken up for discussion
		3 (1) (m)	<p>Relative’ with reference to the owner  Given the fact that relatives under this Act are given access to the PII of the data owner as well as the ability to give consent on his or her behalf when such data owner is incapable of giving consent, we believe that the term should be defined more narrowly.</p> <p>Recommendation:  <b>Specifically, we recommend that the term “relatives” should be restricted till sub-clause (iii) and that the children and grandchildren of the data owner be given preference over the siblings of the owner.</b> In case of absence of the same, a provision may be added to determine the appropriate caregiver, since the Bill already provides for subordinate legislation in this behalf in section 30 (5).</p>	Recommendation to include children/grand children of data owner and limit the Relative definition to sub-clause m(iii)	May be taken up for discussion
		3 (1) (o)	<p>‘Sensitive health-related information’ defining clause.</p> <p>The definition is overbroad at the moment. Given the heavier penalties and obligations that come with use of sensitive health related information, it should be constructed in a manner that is narrow and that clearly delineates what does and does not constitute personal health related information. Further, we would argue that inconvenience or embarrassment is too low a threshold, given the onerous nature of such additional penalties.</p> <p><u>Recommendation</u>  We would recommend the use of a narrow definition which incorporates a list akin to Schedule I of this Bill would be appropriate in this case.</p>	Recommendation provided to define ‘Sensitive health-related information’ to specific details in the context of penalties and obligation provisioned	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		3 (1) (q)	<p>Specified' shall mean as specified by National eHealth Authority of India or State eHealth Authority, as the case may be.</p> <p>Recommendation: We believe the provision should be reworded as follows- <b>“Specified’ shall mean, unless stated otherwise, as specified by National eHealth Authority of India or State eHealth Authority, as the case may be, through regulations made in this behalf”</b> - in order to harmonise the language throughout the Bill.</p>	Recommendation provided for definition of "Specified" to harmonise the language throughout the bill	May be taken up for discussion
		3 (1) (r )	<p>“need to know basis” means the access to digital health data by a specific person for a specific and lawful purpose that is necessary for that purpose or to carry out that function.</p> <p><b>This definition is discretionary in nature and does not provide any guidelines as to what purposes could be construed to be “specific and lawful”. Leaving such an important determination for subordinate legislation, especially when done without guardrails of any kind, could potentially result in the creation of a regulatory loophole and, in the worst case scenario, a subversion of the objects of this legislation.</b></p> <p>Recommendation: In light of our comment, we believe that this <b>definition should be redrafted as an inclusive list of legal purposes with any additional purposes to be added through a notification issued by the Central Government.</b></p>	Recommendation for redrafting of the definition of "need to know basis"	May be taken up for discussion
		4	<p>National Electronic Health Authority of India (NeHA) There is no mention that NeHA will be a corporate body with its own seal and capable of entering into contracts and undertaking obligations on its own behalf. This is contrary to standard practice when drafting legislation for the establishment of statutory bodies. For reference- IWA Act 1985, FSSAI Act 2006, etc.</p> <p>Recommendation: A subsection stating that NeHA is corporate body with its own seal and the power to enter into contracts to be added.</p>	Recommendation provided is addressed under section 5 sub-clause (3)	May be taken up for discussion
		5 (1) (c )	<p>Composition of National Electronic Health Authority of India</p> <p>In this provision, no procedure has been specified for the appointment of these members. This is standard procedure for setting up of independent statutory bodies in order to ensure that records are maintained of candidates and reasons for appointment of members. This in turn ensures that the independence of the body is not compromised. For reference, see section 6 of the FSSAI Act.</p> <p>Recommendation: A section specifying the selection committee for members of NeHA should be added.</p>	Recommendation provided to include "selection committee for members of NeHA"	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
21		8 (1) (c )	<p>Composition of State Electronic Health Authority of India</p> <p>In this provision, no procedure has been specified for the appointment of these members. This is standard procedure for setting up of independent statutory bodies in order to ensure that records are maintained of candidates and reasons for appointment of members. This in turn ensures that the independence of the body is not compromised. For reference, see section 6 of the FSSAI Act.</p> <p>Recommendation: A section specifying the selection committee for members of SeHA should be added.</p>	Recommendation provided to include "selection committee for members of SeHA"	May be taken up for discussion
		19	<p>While the objects of the Act clearly state the establishment of health information exchanges as being amongst them, neither the definition section nor this section define what a health information exchange is. We feel it would be a major oversight to not set out the parameter for determination of what a health information exchange is in the Bill and it could, in the future lead to considerable litigation upon the scope of this Bill.</p> <p>Recommendation: "Health Information Exchange" should be defined. Reference may be made to USA's Federal Trade Commission's May 2014 report on Data Brokers. The said document defines data brokers as follows- "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud."</p>	Recommendation provided for explicit definition of Health Information Exchange.	May be taken up for discussion
		20 (1)	<p><u>Management of Health Information Exchange</u> This section could lead to confusion regarding the correct protocols to be followed and possible engender confusion between the Central Government and NeHA regarding their duties and powers under this Act. Even the sub-sections (2) and (3) do not add much clarity to sub-section (1) since they only demarcate limited areas of regulation. Further, sub-sections (2) and (3) still leave all residual areas to be regulated under sub-section (1), with the attendant confusion over roles of NeHA and the Central Government.</p> <p><u>Recommendation:</u> Therefore, we would recommend that the regulatory roles of the Central Government and NeHA be demarcated in a precise fashion with residuary powers vested in NeHA.</p>	Recommendation provided to provision for regulatory roles of Central Government and NeHA and provision of residual powers	May be taken up for discussion



S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		28 (2)	<p>(2) An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 29 of this Act.</p> <p>Given that no law in India or provision in this Bill defines “generation of data”, it is unclear as to how what the threshold would be for consent for generation. Most actions in a controlled and monitored environment, as many modern clinical establishments are, generate data (some of which would be defined as PII under this Bill). Making generation subject to consent could result in this Bill being borderline unenforceable or becoming a series bureaucratic box-ticking exercises rather than an effective tool to address data privacy concerns.</p> <p><u>Recommendations:</u> All references to “generation” should be removed from the draft Bill.</p>	Recommendation provided for removal of all references to "generation" in context to rights of the owner of digital data specific to give or refuse consent for generation and collection of digital health data	May be taken up for discussion
		28 (8) (d)	<p>(8) The owner of the digital health data shall have, subject to sub-section (1) to (3) above: (d) The right to ensure that in case of health emergency, the digital health data of the owner may be shared with their family members;</p> <p><u>Recommendation:</u> Given that "family members" is not a defined term under this Bill, we believe that the term “relatives” should be used in its stead.</p>	<p>Recommendation provided to replace "family members" with "relative".</p> <p>May be considered after due discussion.</p>	May be taken up for discussion
		29 (1)	It is unclear as to who determines "best interests" in this case. For example, if the child and the doctor of a patient disagreed upon the course of treatment or the continuation of further treatment, who would be the appropriate person to determine “best interests”?	"Best interest". May be discussed	May be taken up for discussion
		29 (5)	<p>Caluse read Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government."</p> <p><u>Recommendation:</u> The Bill should include a definition of "commercial purpose" in order to enable the section to be more inclusive and be able to cover cases not accounted for at present or at the time of specification of such other entities by the Central Government</p>	Recommendation to include definition of "commercial purpose"	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		30 (4)	<p>Any other entity that collects any digital health data shall remain the custodian of such data, and shall be duty bound to protect the privacy, confidentiality and security of such data.</p> <p>We believe that the provision can stand on its own without the use of the word “custodian”, since such word is an undefined term within the Bill itself.</p> <p>All references to the term “custodian” to be deleted from the Bill</p>	<p>Recommendation to remove "custodian" from the clause to maintain clarity May be discussed</p>	<p>May be taken up for discussion</p>
		34(2)	<p>The digital health data collected or stored or transmitted by a clinical establishment or health information exchange, as the case may be, may be accessed by the clinical establishment, on a need to know basis, in such form and manner as may be prescribed under this Act.</p> <p>This definition is discretionary in nature and does not provide any guidelines as to what purposes could be construed to be “specific and lawful”. Leaving such an important determination for subordinate legislation, especially when done without guardrails of any kind, could potentially result in the creation of a regulatory loophole and, in the worst case scenario, a subversion of the objects of this legislation.</p> <p>Recommendation: In light of our comment, we believe that this definition should be redrafted as an inclusive list of legal purposes with any additional purposes to be added through a notification issued by the Central Government.</p>	<p>May be discussed</p>	<p>May be taken up for discussion</p>
		34 (6)	<p>In case of an emergency, certain digital health data shall be immediately made accessible to a clinical establishment, upon a request, including information related to allergies, drug interactions and such other information as may be specified;</p> <p>Emergency is not defined, thus making this provision vulnerable to misuse, especially since there isn't a large body of jurisprudence in India which regulates data rights of persons unable to consent.</p> <p>Therefore, we believe that “emergency” should be defined in a narrow manner so as to limit the scope for abuse of this provision. Reference may be made to Australia's Privacy Act 1988, specifically section 16B of the same as an aid in defining such situations.</p>	<p>Recommendation provided to define "emergency"</p>	<p>May be taken up for discussion</p>
		35 (4)	<p>Without prejudice to the above provisions, a clinical establishment or health information exchange shall ensure through regular training and oversight that their personnel comply with the security protocols and procedures as may be prescribed or specified under this act.</p>	<p>May be discussed</p>	<p>May be taken up for discussion</p>

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		37 (1) (b)	Any person does anything in contravention of the exclusive right conferred upon the owner of the digital health data;  <u>Recommendation:</u> We believe that this clause should make explicit reference to section 31 of the Bill	May be discussed	May be taken up for discussion
		37 (2)	Caluse reads "Any person who breaches digital health data shall be liable to pay damages by way of compensation to the owner of the digital healthcare data in relation to which the breach took place."  We believe that the Bill should include factors that have to be taken into account for the determination of what constitutes appropriate compensation. In the absence of such factors, it would be difficult to put a monetary value on such loss or damage, especially since India does not have a body of jurisprudence around the loss of data as a legal harm.  We would recommend the inclusion of the following factors: <input type="checkbox"/> Severity of breach; <input type="checkbox"/> Sensitivity of data which was so breached; <input type="checkbox"/> If there was any intent or malice behind such breach; If the person who breached such data also broke a duty of care to data owner; <input type="checkbox"/> Measures taken by the person to remedy the breach, if any; <input type="checkbox"/> Quantum of financial loss suffered by the data owner(s), if any.	Recommendation provided include factors for determination of the what constitutes appropriate compensation.  May be discussed	May be taken up for discussion
		41 & 42	<del>Obtaining the digital health information of another person</del>  It is unclear as to why there are two separate offences prescribed for what, effectively, are the same set of actions i.e. the unauthorized access to digital health data/information of a person by another person.  We would recommend the merger of these two separate sections into a single offence, with the higher penalty being attached to malicious intent.	Clause 41 refers to the person whereas Clause 42 refers to the digital health Data.  May be discussed.	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
		45 (3)	<p>Notwithstanding anything stated in sub-section (2) above, if the data breach is notified, no complaint is maintainable after two years from the date of such notification;</p> <p>There are no requirements for notice under this Bill. Therefore, there are no safeguards in place to ensure that a company will notify data owners in an accessible manner or in a manner that enables a proper understanding of the need for their data, the consequences of collection, storage and breach, their remedies in case of misuse or breach of their data, and of alternative methods (if applicable). For example, a company notifying a man unable to read English in an English language notification or posting notices in a place or manner that is inaccessible would clearly result in the consent being given not being based on a proper understanding of the issues involved.</p> <p><u>Recommendation</u> Therefore, we would recommend that a provision be added which adds the following conditions for a notice:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Mentions specific details of data that was breached or damaged or destroyed; l</li> <li><input type="checkbox"/> Placement accessible to each data owner;</li> <li><input type="checkbox"/> Use of concise, clear and easily understandable language;</li> <li><input type="checkbox"/> Mention of consequences of such breach for the data owner, specific measures being undertaken to deal with such breach</li> <li><input type="checkbox"/> Use of audio-visual and other appropriate means for notifying such data owners as are unable to read.</li> </ul>	<p>Recommendation for provision on safeguards in place to notify data owner.</p> <p>May be discussed</p>	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
22	<a href="#">Dr. CS Buch</a>	Clause 5	Please find the Reference Para and Suggestions as detailed below (iii) One from Law &/or Cyberlaw (iv) Law or Cyberlaw Request to abbreviate it to SeHat instead of SeHA ...AuthoriTy please ALL occurrences of 'law' should be accompanied by cyberlaw where compatible	Suggestion to include Cyberlaw along with Law wherever applicable	May be taken up for discussion
		Chapter V Offences and Penalties	<p>The punishment for similar hacking in Indian IT Act is as follows which we know.....            "Section 65 in The Information Technology Act, 2000            65. <i>Tampering with computer source documents.</i>-Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation.--For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."</p> <p>Can it NOT lead to a discrepancy? Or some misinterpretation by me about applicability?            Also Person like Doctor or Lab or Hospital who are trying to HELP the patient by providing care may be unnecessary target of punishment in the event of someone trying to hack the system. When a hack has been confirmed and the data has been stolen the person who does it is charged with One YEAR imprisonment inspite of the motive being criminal in Cyberlaw and Cybercrime whereas the parties trying to HELP are having punishment of 3 years imprisonment. Some way has to be decided between occurrence by mistake and deliberate attempt by non healthcare worker attempting crime and am sure it can be thought about and worded by our esteem Legal Consultants</p>	Suggestion to harmonise any discrepancy in offences and penalties under the proposed Act with that of Information Technology Act , 2000	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
23	<a href="#">Harvard medical School</a>	NA	<p>We write to you on behalf of a team of medical practitioners, academics and policy makers from India and the US, who have collaborated to draft a response to the proposed DISHA law.</p> <p>Our team has provided extensive inputs the Justice Shrikrishna Commission's White Paper on Data Protection, with a focus on HEALTH data.</p> <p>The responses can be found here: <a href="https://cdn2.sph.harvard.edu/wp-content/uploads/sites/5/2018/02/RHarvard-FXB-Responses-to-WP-Health-Data-FINAL.pdf">https://cdn2.sph.harvard.edu/wp-content/uploads/sites/5/2018/02/RHarvard-FXB-Responses-to-WP-Health-Data-FINAL.pdf</a></p> <p>We hope you find them helpful.</p>	Provided Comments that is already submitted to Justice SriKrishna committee on Data protection law	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remarks	Remarks
24	<a href="#">Ankita Sankala</a>	1. Caluse 10/3 4. Caluse 5 & 9	<p>DISHA Act is very nicely written and it covers almost everything. But, While going through the draft of DISHA Act I found it suitable but there are couple of points on which I think team have to revisit one more time.</p> <p>1. Reappointment of chairperson as required in section 10(3). Reappointment should be restricted to two terms otherwise it will become full time employment of one person and it may affect the independence of a person. And also if position get rotates then there may be a chance that new chairperson may come with new possibilities and one person is not taking advantage of his/her position. Moreover the appointment of chairperson should not be politically influenced rather be it rational.</p> <p>2. If someone alters the health data of owner for personal benefit then what are the consequences and penal provisions on that person who alters the data.</p> <p>3. I think there is lack of strict provisions on health insurance companies as they are also holding and sharing personal data of owner.</p> <p>4. Powers of chairperson as specified in section 9. I think both bodies whether central or state should be from government influence. As government is keep on changing with every election and this will effect the working and independence of chairperson</p>	<p>1. Provisions in Clause 10/3. May be discussed</p> <p>2.Provision in Clause 37 Breach of digital health data</p> <p>3. Health insurance companies are regulated by IRDAI under IRDA Act 1999.</p> <p>4. Addressed through Provision in clause 13 - Temprorary association of persons with Natonal or State Authorities for particular purposes</p>	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
25	<a href="#">ICMR NCDIR</a>	1/3e	To include information collected; a. Surveys/research studies b. Part of regular health system functioning in public and private sector at all levels c. By non-health agencies/departments eg. Census, mortality data by ORGI d. The process of creation of Digital health data is not completely defined. As Digital health data can be created / generated in several ways , it is crucial to explain if the Act is restrictive to Electronic Health Records created/ generated during the process of health service provision or it would include health programme implementation, monitoring, surveillance , or health/medical or clinical research; OR health data generated by individuals through wearable devices or apps and stored by other service providers	Suggestion for Provision in Clause 1/3e	May be taken up for discussion
		1/3f.	a. Entity- health research organizations are not included b. Jurisdiction of the Act in terms of coverage : private/ public institutions covered ; companies/organisations that develop, maintain, implement the software for generating such Electronic health records or Digital health data should also be explained	Suggestion for Provision in Clause 1/3f	May be taken up for discussion
		1/3h.	A disease registry or National programme on disease surveillance or monitoring can be considered as Health information exchange	Suggestion for Provision in Clause 1/3h	May be taken up for discussion
		1/3i.	Clinical establishments should also include; a. Health wellness/promoting centers b. Information collected during camps/special drives/promotional events	Suggestion for Provision in Clause 1/3i	May be taken up for discussion
		1/3j.	Rights of the owner of data may be in sync with international guidelines ( General Data protection rules of EU and the proposed Data protection Act proposed) . But the reality of consent processes in routine health care provision need to be contextualized and the rules of Rights of owner of data have to be explained. In most instances, it will be the Doctor or Hospital that collates EHR information for further analysis or interpretation who will be responsible for maintaining privacy, confidentiality. <b>The rights of this immediate group of personnel – roles, responsibilities and safeguards should be explained.</b>	Provision in Clause 22. Powers and functions of NEHA	May be taken up for discussion
		1/3o.	Definition of Sensitive health related information should encompass all that is identified as 'personal identifiable information' and , in combination with other details pertaining to individuals, 'that if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, violence, discrimination or unfairness to an individual'. The present definition is incomplete as it does not specify all personal identifiable information. IT rules The IT rules 2008 specify that sensitive personal information includes 'medical records' . While DISHA Act defines 'sensitive health information' based on impact to individual. It is problematic to understand who will determine that there could be an impact if there is a breach/compromise in confidentiality and privacy	Provision in Caluse 1/3o is observed in context to Provision in IT Act 2008 amendment in Caluse 3	May be taken up for discussion



		2/5	NeHA membership should also include 1 Clinician of repute who can understand and guide clinical scenarios in information collection, storage, usage etc and 1 ex officio member from DHR/ICMR to represent the health research community who not only generate but also use available health data for research purposes.	Provision in caluse 5 does. May be discussed	May be taken up for discussion
		3/22 (1) a.	Should include formulation of guidelines for analysis of data also since data collected for any purpose by anyone is deemed to be analysed unless otherwise stated	Provisioned in Caluse 29 (g)	May be taken up for discussion
		4/29 (1)	<p>a. Add item i- to facilitate disease surveillance for public health actions</p> <p>b. Personal identifiable information is also used for research and public health purposes. The present Act is restrictive in this sense by stating that 'that for public health related purposes mentioned in clauses (d) to (h) of sub-section (1), only de-identified or anonymized data shall be used, in the manner as may be prescribed under this Act'</p> <p>c. Thus, the ACT should apriori state instances / purposes where personally identifiable information may be used for public health purposes – as in registry, disease surveillance with provision of safeguards for data protection and privacy of individuals. There should be scope for further revision of the purposes/r organisations that can handle personal identifiable information within the Act.</p> <p>d. The processes of data protection need to further explained. There has to be reference to the Data protection bill that is in the pipeline.</p> <p>e. The present statutory or legal requirements that exist for access and disclosure of personally identifiable information can be stated. This can also include point 'c' above, where in organisations involved in such collection of data for purposes of Registry or disease surveillance or mortality statistics as mandated are already collecting such information.</p>	Suggestion for purpose for collection, storage, transmission and use of digital health data	Covered under the Act. Refer Clause 29/1
		4/29 (4)	<p>a. Identifiable data is needed by disease registries to clean raw data to avoid over counting of same person for same health indication more than once for the same health event, as these will overinflate health statistics. However, the identifiers are not to be used for analysis and reporting.</p> <p>b. Provisions for sharing the identifiable data must be laid down</p>	De-identified and anonymised data shall be used for public health related puposed. Refer Clause 29 (1)	Covered under the Act. Refer Clause 29/1

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remarks	Remarks
26	<a href="#">NASSCOM</a>		<p>This is with reference to the draft Digital Information Security in Healthcare, Act (DISHA) which was published on 21st March 2018.</p> <p>At the outset, we thank Ministry of Health and Family Welfare (MOHW) for inviting industry comments on the same, however, given the potential impact of this law on large number of companies, <b>we request you to kindly consider extending the timeline for sending inputs by at least 6 weeks</b> enabling us to suitably discuss with various stakeholders and share a detailed response.</p> <p>Further, data protection committee chaired by Justice B.N. Srikrishna has been mandated to develop the data protection framework and draft legislation for the country. There would be significant overlap on areas related to healthcare data, and we would therefore suggest that various definitions such as personal data, sensitive personal data, and adjudication processes maybe suitably harmonised and synergised between DISHA and the awaited Data protection framework.</p> <p>While we will share a detailed response to the draft DISHA, we would also suggest DISHA be finalised only after the data protection framework is finalised, or the DISHA should provide for option to harmonise as and when the DP law is announced.</p> <p>We look forward to your support.</p>	Request for extension of time for submission of comments	No action

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
27	<a href="#">Heartcare Foundation</a>		<p>The undersigned is the President of the registered trust Heart Care Foundation of India which has its registered office at E-219, Greater Kailash – II, New Delhi. The said registered trust is a charitable and non-profit organisation. Heart Care Foundation of India (hereinafter referred to as “HCFI”) is registered charitable trust which was incorporated in the year 1986 for creating awareness about all aspects of health using innovative low cost informative ways. In two of its events, one Run for the Heart in 1991 and Perfect Health Mela in 1993, Government of India has released National Commensurate Postal Stamps. Also, in 2012 Government of Rajasthan released Cancellation Stamps for organizing first ever telemedicine camp. Also, for organizing Mega CPR Camp, the HCFI’s name has been recorded in Limca Book of Records. The National President of HCFI has been honoured with the highest national award “Padma Shree” in the year 2010.</p> <p>The undersigned has gone through the Digital Information Security in Healthcare, Act (DISHA) which is open for public consultation and comments. The undersigned would like to give some suggestions on the said bill which are annexed herewith.</p> <p>There is no requirement of enacting this DISHA as already there is one central Legislation namely "The information Technology Act, 2000" (hereinafter referred to as IT Act, 2000) which was enacted by honorable Parliament of India</p>	Reference to already existing ITA 2000 provided and suggesting no need for the proposed Act	The ITA 2000 / Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
28	<a href="#">George Institute</a>		<p>The term "Owner of Digital Health Data" would benefit from being defined clearly, in the current version of the document it has been used interchangeably across multiple stakeholders. We recommend that any person whose data is being transformed into a Digital Health Record be defined as the Owner.</p> <p>Similarly, we propose that "<b>Generator of Digital Health Data</b>" could be considered. Any person, establishment or entity that generates Digital Health Data be included as the Generator. This therefore the definition would include other stakeholders beyond clinical establishments, <b>such as Public Health and Research Institutions who generate digital health data for purposes other than provision of clinical care.</b></p> <p>We propose that a unique identifier such as ADHAR be defined as the primary index for the digital health information exchange (HIE), it would also be important that generation of digital health data. However, the non-availability of an Unique ID should not a deterrent from a person availing essential healthcare services for want of generation of digital health records.</p>	<p>Suggestion for definition of "Owner of Digital Health Data" and "Generator of Digital Health Data".</p> <p>"Owner" is defined in Clause 3 (j)</p>	May be taken up for discussion
		Chapter 4 / 28 / 2	<p>Clause reads " Data owner has right to give or refuse consent for the generation and collection of digital health data"</p> <p>Further clarity on the consenting process would be necessary</p> <p>The timing of the consent and format for the same to be defined</p> <p>Is the consent taken once for each data owner / patient or does the consent have to be repeated at each encounter?</p> <p>Format: Whether the consent should be on paper, signed by patient and his relative or would an electronic consent suffice?</p> <p>Recommendation : DH platforms to maintain an audit trail of the consent for digital data generation.</p> <p>The data owners to be provided an option at the time of registration to opt in for consent to be carried forward through multiple episodes of</p>	<p>Suggested elaboration of term "Consent" for clarity. May be discussed</p>	May be taken up for discussion
		Chapter 4 / 28 / 3	<p>Owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data</p> <p>Consent should incorporate feature to opt out for storage and /or transmission of data, incorporating a mechanism to ensure that storage and transmission functions are disabled for those opting out</p> <p>A log of the opt out to be maintained</p>	<p>Suggestion provided for Consent of owner to have opt out facility affecting storage, transmission of data. May be discussed</p>	May be taken up for discussion
		Chapter 4 / 28 / 7	<p>Owner of the digital health data shall have a right to access their digital health data</p> <p>Recommendation: Timestamping the download of the dataset by the owner might be important to ensure that any data breaches while the data is in the custody of the data owner would not be attributed to the data generator</p>	<p>Suggestion for security of digital health data of owner</p>	The authority shall provide necessary details guidelines and standards for security compliance

Chapter 4 / 28 / 8 b	<p>Right to require their explicit prior permission for each instance of transmission or use of their digital health data in an identifiable form</p> <p>Recommendation: that the patient / owner provides approval for access to their identifiable data by their nominated care providers. Requiring prior permission for every use or transmission is a significant time and cost impact. The approval could have an expiry time on it to prevent infinite approvals.</p>	Suggestion for seeking permission from health data owner for access to identifiable data.	May be taken up for discussion
Chapter 4 / 28 / 8 c	<p>establishment</p> <p>Recommendation:</p> <p>At each instance where digital health data that includes personal identifiable information is accessed, an audit log is available for the patient/owner to see electronically the digital identity.</p> <p>We also recommend incorporating proactive notifications, is only done for new care providers that haven't been previously authorized. This provides a better balance of protecting the patients and minimizing the administrative burden of handling calls into the system.</p> <p>Further, we recommend that the ACT outline the mechanism of notification: Notification on patients mobile / email to patients email ID</p> <p>Would there be a need to track if the notifications have been delivered/ read/ acknowledged.</p>	Suggestion for provision of notification mechanism to data owner	Implementation issue. The authority shall provide implementation guidelines
Chapter 4 / 28 / 8 d	<p>In case of health emergency, the digital health data of the owner may be shared with their family members</p> <p>Recommendation:</p> <p>Incorporating a 'break glass' provision that enables the emergency care providers to access the information. Waiting on the family to get this information may not be feasible in emergencies. Post the event, reviews can occur to ensure the 'break glass' event was reasonable given the known information at that time.</p> <p>We suggest the act outline if there is a requirement by the CE / DHD generator to confirm identity and relationship of the family members as per definition in 3(1)(m) before sharing the digital health data.</p>	Suggestion for health emergency.	May be taken up for discussion
Chapter 4 / 28 / 8g	<p>Right to seek compensation for damages caused by a breach of digital health data</p> <p>Recommendation :</p> <p>Specifications for data transmission integrity standards to be outlined in the act to ensure uniformity of compliance, DH Generators to demonstrate adherence to the specifications outlined</p>	Provisioned in Clause 22 may be referred to. Powers and functions of NeHA.	May be taken up for discussion

Chapter 4 / 29 /1	<p>Digital health data may be generated, collected, stored, and transmitted by a clinical establishment and; collected, stored and transmitted by health information exchange.</p> <p>We suggest that identifiable data can be held by clinical establishment or parties that the patient / owner authorizes.</p> <p>We recommend broadening the definition of DH data generators to include public health and research organizations and software firms acting for clinical establishments to collect/store the data.</p> <p>We also recommend that entities that generate Digital Health Data to be pre-registered under DISHA act and be provided an Unique Entity identifier so as to ensure only authorized entities are generating and exchanging Digital Health Data</p>	Suggestion for holding of identifiable data and definition of Digital health data generators	May be taken up for discussion
Chapter 4 / 29 /1	<p>owner of the data. Public health related purposes only de-identified or anonymized data shall be used</p> <p>Recommendation : It would be important to define direct care , providing community based screening that results in diagnosis of hypertension or diabetes is a precursor to clinical care at a clinical establishment , it might be necessary for the purpose of the screening to include some personal identifiers to efficiently refer the persons into health facilities.</p> <p>Further to ensure continuum of care community based healthcare providers when approved by the patients should be considered as approved care team.</p> <p>The Act needs to create an enabling environment to ensure communication between the doctor and pharmacies/specialists/hospitals can occur in a seamless way. We further recommend that direct care can include preventative care to the patients by the care provider.</p>	<p>Suggestion to define direct Care.</p> <p>May be discussed.</p>	May be taken up for discussion
Chapter 4 / 29 /5	<p>Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government.</p> <p>We suggest that the act clarify 'commercial purpose'.</p> <p>Further we recommend that the act needs to be clear about what constitutes a commercial purpose and a list of commercial purposes be prespecified.</p> <p>Would electronic health software that can access the record be at risk here or e-prescription software that sends the script from the doctor to the pharmacy.</p> <p>We recommend "the digital health data must not be disclosed to any person outside the current approved care team or only with explicit patients / owner express consent"</p>	Suggestion to define "Commercial purpose"	May be taken up for discussion

Chapter 4 / 30 /2	<p>Consent from the owner, recorded in the form and manner as may be prescribed under the Act A copy of the consent form to the owner</p> <p>Recommendation : that the act provides a framework/ template for the consent and also consider provision for the same to be tracked electronically than on paper.</p>	<p>Suggestion to provide template for Consent.</p> <p>Cluase 22 may be referred to. Powers and functions of NeHA.</p>	<p>Implementation issue.</p> <p>The authority shall provide implementation guidelines</p>
Chapter 4 / 33/2	<p>Transmit the digital health data to the health information exchange securely, in an encrypted form, after retaining a copy for reasonable use by the clinical establishment</p> <p>Recommendation : that the encryption protocols to be used by the CE / DH Data generator is prespecified and regularly updated to ensure compatibility and compliance to the protocols outlined for the HIE ( IHIP)</p>	<p>Clause 22 may be referred to. Powers and functions of NeHA</p>	<p>Implementation issue.</p> <p>The authority shall provide implementation guidelines</p>
Chapter 4 / 36/1	<p>An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed</p> <p>Recommendation : that the act define the mechanisms for the review process of data accuracy by the data owners.</p> <p>We suggest that a link to view and comment on the data be provided through a secure mechanism and if the link is not acted up within a specified period , it would be deemed approved with no inputs required for edits.</p>	<p>Clause 22 may be referred to. Powers and functions of NeHA</p>	<p>Implementation issue.</p> <p>The authority shall provide implementation guidelines</p>
Chapter 4 / 36/2	<p>Rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.</p> <p>Recommendation : that an electronic logging mechanism for such data edit requests, tracking the timelines and responding on action taken be incorporated by the CE/ DH Data generators</p>	<p>Clause 22 may be referred to. Powers and functions of NeHA.</p>	<p>Implementation issue.</p> <p>The authority shall provide implementation guidelines</p>
Chapter 4 / 38/2	<p><del>Any person who commits a serious breach of health care data shall be</del> punished with imprisonment, which shall extend from three years and up to five years; or fine, which shall not be less than five lakh of rupees.</p> <p><b>We note with concern that the legal implications outlined in the act would be huge disincentive towards generation of electronic health records and likely derail the ambitious IHIP vision. CEs are likely to refrain from encouraging the patients to opt into Digital Health Records.</b></p> <p>The Act should consider providing an enabling environment for preventing data breaches through proactive measures.</p>	<p>Suggetion for enabling environment for preventing breaches through proactive measures.</p>	<p>May be taken up for discussion</p>
Schedule 1	<p>Personally identifiable information</p> <p>Comments: The personally identifiable information list would benefit from being redefined. Medical records and history are to be excluded from personally identifiable information as it would be required for public health purposes.</p>	<p>Suggestion for definition of Personal Identifiable Information.</p>	<p>May be taken up for discussion</p>

## 909695/2018/E-GOVERNANCE

		<p>New Issue :</p>	<p>We should not disallow direct sharing of identifiable data for direct patient care between two hospitals.</p> <p>Recommendation :</p> <p>In the instance of authorized referral for direct patient care, digital health data maybe exchanged in encrypted format, subject to the owner / patient having opted in for data sharing.</p> <p>In the case of life threatening emergencies, the provision of care should not be hampered by non-availability of critical digital health data for prompt decision making. It is further recommended that a minimum dataset for emergency access be defined (eg. Blood Group, Drug Allergies, Special conditions such as Hemophilia, G6PD deficiency etc.), a provision of authorization of access to minimum dataset should vest with a designated delegated authority within each clinical establishment.</p>	<p>Suggestion for sharing of digital health data for direct patient care and emergencies.</p>	<p>May be taken up for discussion</p>
--	--	--------------------	---	---	---------------------------------------



S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
29	FICCI		<p>Digital India and Startup India are key initiatives of our Honorable Prime Minister with a vision to transform the country into a digitally empowered society. It aims to empower citizens to avail all the services including healthcare with more ease and convenience. The vision of better, simpler, regulations for businesses will foster entrepreneurship and in turn will accelerate innovation in the healthcare. Accessibility, affordability and lack of awareness are the major challenges in the healthcare sector. These barriers could be effectively overcome by adopting technology into the healthcare system. Health-tech startups have been innovating to improve healthcare services and make it more affordable and accessible for the patients.</p> <p>These companies apply advance technologies like artificial intelligence and machine learning on healthcare data to provide better services. There is an urgent need to nurture this promising sector with the right set of policy frameworks and guidelines in order to provide the benefits that the sector fosters for the consumers.</p> <p>Keeping this in view, please find enclosed our specific concerns in the draft DISHA regulations. While the intent and the proposed are in the right direction and well intentioned, we have concerns and suggestions for the following points</p>	NA	-
			<p><u>Phasic implementation of DISHA and Ease of doing business for Healthcare startups</u></p> <p>DISHA Draft has failed to recognize the value of Health-tech startups in the ecosystem and has restricted their ability to innovate for the benefit of the patients and providers. DISHA Draft needs to explicitly recognize the role of Health-tech startups and empower them to handle digital health data to drive innovation and access in the healthcare sector.</p> <p>We recommend that the above regulations should be implemented in phasic manner and in first phase it should be only be applicable for clinical establishments and health exchanges and not for digital health startups.</p>	Recognition for innovation based health entities. May be discussed	Implementation issue. The authority shall provide implementation guidelines
			<p><u>Prohibition of commercial use of even anonymized and de-identified data</u></p> <p>Data analytics on anonymized and de-identified data is a legitimate commercial activity that can create tremendous value in health care ecosystem without putting any consumer's privacy at risk. Prohibition can be specifically prescribed for some activities like sale of patient data to any third party.</p> <p>By prohibiting any commercial use of even anonymized data will impact innovation in healthcare sector and disrupt the business model of many existing digital health companies. Further, it will impact the potential of advanced technologies for chronic disease management.</p>	<p>Use of anaonymised and de-identified data to create value in health care and legitimate commercial use.</p> <p>Caluse 29/5/</p> <p>May be discussed</p>	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<p><u>Disproportionate sanctions and uncapped penalty</u></p> <p>The sanctions prescribed under 38 and 42 extend to imprisonment and there is no requirement to establish the wrong intent. This will lead to undue harassment for some administrative slips without any wrong intention. Further, it will discourage the entry of new entrants in this space.</p> <p>Serious breach is very broadly defined and needs more practical and reasonable definition.</p> <p>We recommend it to be suitably amended to include only the civil liabilities, the need of establishing the wrong intent and the penalties should be reasonably capped.</p>	Provision in Clause 38. May be discussed	May be taken up for discussion
			<p><u>Expectation to own the servers for storage of digital health data</u></p> <p>The digital service providers will not maintain technology infrastructure for storage and hence it is reasonable to deem that these operations are likely to be outsourced to say, server management companies. Assigning these responsibilities on Digital Service Providers will additionally burden them with unnecessary operational costs. Further, seeking Digital Service Providers to 'own' such medium of transmission will lead to an impractical scenario. We recommend that this needs to be deleted.</p>	Provision in clause 31	Implementation issue. The authority shall provide implementation guidelines
			<p><u>Right not to be refused Health Service</u></p> <p>A digital health service provider will not be able to provide health service if the data owner refuses to give consent for generation, collection, storage, transmission and disclosure of his/her health data. Moreover, there are regulatory compliances under existing laws to maintain the record in some particular conditions. We believe this is unreasonable and hence should be deleted.</p>	May be discussed	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
30	Max Healthcare		Would like to introduce myself - I am Sumit Puri, CIO, Max Healthcare. Thanks for the opportunity provided to share our initial comments on the proposed DISHA act. We have gone through the draft and must say that based on our initial perusal, the Act in its present form will have <b>adverse effect on patient safety and Govt efforts</b> to improve electronic health record compliance by healthcare providers. There are <b>myriad restrictions specified on sharing of anonymised data, mandated ownership of servers/ storage etc.</b> by healthcare providers and <b>right to withdraw consent</b> by patients , which could impact patient safety research efforts, have medico legal implications of misuse for insurance etc. and add to costs and management overheads, especially for small and medium sized healthcare institutions. Am enclosing some key concerns below for your reference -	Concerns on restriction in Sharing of Anonymised data, ownership on storage affecting patient safety and digitisation efforts	May be taken up for discussion
			<p>Key Challenges:</p> <p>Right to refuse / withdraw consent.</p> <p>Section 28 of DISHA provides that an owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, and right to refuse or withdraw consent for the storage and transmission of digital health data.</p> <p>Submission:</p> <p>In case of refusal by a patient for generation and collection of digital health data at the time of admission, it seems the hospital has to keep the health record in physical form only. It would be difficult for corporate hospitals and healthcare providers who generally maintain the medical records in electronic form only. Similar issues would apply in case of withdrawal of consent by a patient later as <b>storage of medical records for a period of 3 years is specified in MCI guidelines</b> and there are laws which provided for a longer period also. <b>Right to refuse /withdraw consent should ideally be deleted as it would be practically and technically difficult to remove all the traces of digitised medical records from the myriad IT systems.</b></p> <p>Anonymised or de-identified data</p> <p>DISHA allows anonymised or de-identified data to be used for specific public health purposes including for early identification and prevention of diseases and research for public health, clinical and academic purposes. However, it strictly prohibits access, use or disclosure of DHD (whether in identifiable or anonymised form) by any other entity for a commercial purpose.</p>	right to refusal by owner and technical difficulty involved for CE and in reference to MCI guidelines. May be discussed	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remarks
31	Intel		1. Achieving very large scale interoperability of digital health systems is notoriously complex and requires careful planning, coordination and execution. Moreover, consulting with relevant healthcare stakeholders (clinical establishments, industry, local and State actors, healthcare professionals and patients' representative organisations) has proven to be a critical activity in similar initiatives. For this purpose, we suggest the creation of a DISHA Advisory Committee. This committee, composed of stakeholder organisations representing the several intervening classes of actors involved in the implementation and usage of eHealth as covered by this plan, would be called to advise the National Electronic Health Authority at least during the formulation and selection of standards, and the design and implementation phases of the Health Information Exchanges.	Suggestion for creating DISHA Advisory committee considering the complexity involved in the large scale system	May be taken up for discussion
			2. We would also like to raise some comments and provide suggestions on the proposed data related sections of the DISHA. <input type="checkbox"/> As India is readying itself for a holistic data protection law, it matters to consider the potential inter-relations with DISHA. Will they overlap, complement or conflict with each other? These are crucial and complex issues that solicit a reflection by the MoHFW before finalizing DISHA.	inter-relations of the proposed Act with holistic data protection law	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.
		Section 28(3)	3. Section 28(3) – In some circumstances, withdrawing consent may be problematic or even impossible or could involve a disproportionate effort, in particular when processing health data for scientific research. There should be an exemption from withdrawing consent when such is impossible or seriously impairs the achievement of the objectives of that processing	withdrawing of consent and complexity involved	Implementation issue. May be taken up for discussion
		Section 28(8)(b) and	4. Section 28(8)(b) and (c) – The requirements in this section may become impractical to implement. When the right to require (b) explicit prior permission for each instance of transmission or use of their digital health data or (c) to be notified every time their digital health data is accessed by any clinical establishment is exercised by the data owner. Consider a general practitioner asking advice from a specialist - how would that work in practice? There should be an exception to the application of this right at least when one of 29(1)(a), (b) or (c) is met and ideally when any of 29(1) is met.	Consent of owner for each instance and concerns involved.	Implementation issue. May be taken up for discussion

		Section 29(5)	5. Section 29(5) - Anonymised digital health data should not be approached in the same way as non-anonymised digital health data. <b>The data owner should be able to give consent to the use of his/her anonymized health data for research - commercial or not. Moreover,</b> the data owner should be able to have the possibility to give consent to the processing of his/her health data irrespectively of it being identified, de-identified or anonymized, for research or otherwise, for commercial purposes or not - as long as the rights set on Section 28 are met (considering the comments above). <b>The MoHFW is right to be concerned that the potential for abuse by some entities (e.g. insurance companies, employers) may impact individuals negatively when these entities have access to sensitive digital health data.</b> To eliminate these risks, there should be an explicit prohibition of the use of digital health data for the purpose of health insurance and employment (or other purposes as the Government may specify) in any way that adversely discriminates the data owner, or as the law mandates. Still, <b>consent for specific purposes should be the basis</b> upon which digital health data is made accessible, or when there is a statutory or legal requirement to access or disclose information.	Consent for specific purpose as a basis for accessing digital health data	May be taken up for discussion
		Section 30(2)(c) and	6. Section 30(2)(c) and (d) - It should be clarified what <b>"identity" means</b> . Is the term related with actual names of individuals or does it refer to specific roles/classes of (healthcare) practitioners, or both?	May be discussed	May be taken up for discussion
		Section 31(4)	7. Section 31(4) – There seems to be an obligation to host digital health data in the premises of clinical establishments or health information exchanges. Considering the varying levels of digital preparedness of clinical establishments (e.g. single doctor practice vs large hospital) there may be good reasons to allow for digital health data to be hosted by recognized and specialized IT third parties (e.g. cloud computing service providers). Cloud service providers are specialized entities that by the scale of their activities can provide a high level of data security. As long as the provisions of DISHA are met they should be considered for the purpose of storage and transmission of digital health data.	Concern expressed in obligation to host digital health data in CE/ HIE. May be discussed	Implementation issue. May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remark	Remark
32	ClearMedi Healthcare		<p>First of all I must appreciate that govt of India has taken bold step to secure healthcare data of the country and coming up with new act "DISHA". Please find my comments or question which should be answered in this act.</p> <p>Ownership of data: Patients, State, Hospital Who can generate this data: Hospital, clinic, laboratory, diagnostic center, Who can use this data: doctor, patient, hospital, research org, pharmaceutical company with consent of patients. Who can sell this data: patients, hospitals &amp; clinic.</p> <p><b>Data is in which form : digital or hard copy or voice</b></p> <p>Validity of data: Old or new or fresh; Categorisation of data: Of low, moderate, high importance</p> <p>Cost of data: high, moderate, low ; Significance of data: Confidential, Restricted, Urgent</p> <p>Leakage of data or theft definition; Punishment of theft of data: Criminal law</p> <p>Compensation of misuse of data; Royalty for better use of data for growth or invention: Hospital &amp; patient</p> <p>Volume of data transaction</p> <p>Cyber security of data</p> <p>Registration of data owners with unique identification number or bar code</p> <p>Language of data: ?</p> <p>DE codification of data</p> <p>Direct or indirect data</p> <p>Age of data</p> <p>Vulnerability of data</p> <p>Law of transfer of data ownership</p> <p>Data renting</p> <p>Data transaction authority</p> <p>Ministry of healthcare Data security</p> <p>Complaining authority</p> <p>IPC Code; Jurisdiction ;Data tracking system; Data distortion</p> <p>Inclusion in MCI Or NMC act for medical ethic &amp; etiquette</p>	Most of the concerns raised are addressed implicitly focussing on Digital Health Data Security, privacy, patient care throughout the draft Act	Most of the concerns raised are addressed in the Act  Privacy of Health Data in paper / hard copy format is dealt under MCI Act
			<p>Beside this Top 10 Tips for Cybersecurity in Health Care</p> <ol style="list-style-type: none"> <li>1. Establish a Security Culture</li> <li>2. Protect Mobile Devices with tracker</li> <li>3. Maintain Good Computer Habits</li> <li>4. Use a Firewall</li> <li>5. Install and Maintain Anti-Virus Software</li> <li>6. Plan for the Unexpected</li> <li>7. Control Access to Protected Health Information</li> <li>8. Use Strong Passwords and Change Them Regularly</li> <li>9. Limit Network Access</li> <li>10. Control Physical Access</li> </ol>	Suggestion provided for Data security	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
33	Invest India		<p>RECOMMENDATION ON ADDRESSING AND PROVIDING CLARIFICATION ON SECOND-ORDER DERIVATES OF HEALTH DATA</p> <ul style="list-style-type: none"> <li>• Description: The act is comprehensive in its coverage on areas of collection, storage, and transmission of Health data. However, the act does not address the area of second-order derivatives: products built using health data. This lack of definition leaves a lot of ambiguity around the ownership, usage, transfer and sale of such products.</li> <li>• Definition: Here, by second-order derivatives of Health data, we refer to software, products and algorithmic models that are created using health data and only contains elements of health data that is necessary for the product to work. Additionally, any health data contained in the product cannot be linked back to any individual.</li> </ul>	May be discussed and considered	May be taken up for discussion
			<ul style="list-style-type: none"> <li>• Why this is important: India has 250+ Venture capital backed Health technology startups. Many of these are attempting to create solutions that could benefit different disease areas that the Indian population struggles with.</li> <li>Health- data based start-ups often produce innovations that can increase reach of healthcare while reducing the costs. Such innovations could help the Indian healthcare system increase reach in a cost-effective manner.</li> <li>Promoting health Innovation has proven to be beneficial in other regions. For example, the FDA just approved a diagnostic system that autonomously analyzes images of the retina for signs of diabetic retinopathy- IDX-DR. This system could significantly increase the reach of such tests at a minimal cost as the product is autonomous and not dependent on a doctor. Such systems are built on algorithms derived using anonymous health data. For such innovations to be encouraged it is important to allow the transfer, use and sale of second-order derivatives of health data.</li> </ul>	NA	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
34	CARING Dr. Vidhur Mahajan		<p>I believe the comments would be helpful as I am a medical graduate (M.B.B.S. from L.T.M. Medical College, Mumbai) and MBA in Healthcare Management (from The Wharton School, USA) and have extensive experience of handling large number of patient records while running Mahajan Imaging Pvt. Ltd., India's leading chain of medical imaging centres and its research and development arm called C.A.R.I.N.G. - Centre for Advanced Research in Imaging, Neurosciences and Genomics.</p> <p>Below are my comments:</p> <p>1. Chapter II, Point 5, 6, 8 and 9 Given that India has, over the past few decades, established itself as an IT hub for the world, I believe it would be worthwhile to consider having some representation from the private sector in the National and State Health Authorities and Executive Committees. With all humility I wish to state that the Government has limited experience of developing, implementing and maintaining digital health record systems and having support from leaders in the private sector, many of whom are multi-national companies whose products are used the world over, would be a useful addition to the teams.</p>	Provision in clause 5 & 8 Comment addressed in Clause 13.	<p>Covered in the Act through Temporary association of Persons with National or State Authorities (Clause 13).</p> <p>May be taken up for discussion</p>
			<p>2. Chapter III, Point 23(1) and 25(1) While it is important that the National and State Authorities have visibility into the functioning of the digital health exchanges and the clinical establishments, there has to be some provision to prevent the National and State Authorities from viewing patient-specific information as otherwise it would be in breach of patient confidentiality. It is also good that the Act explicitly states that there would be "no or least possible hindrance" to the normal working of the establishment, it would be better to define service levels and expectations beforehand so that establishments take appropriate steps. In other words, having specific guidelines laid out at the very start would be much better. It would also be important to define the composition of the team that would carry out these inspections and it is requested that the team includes representation from the clinical domain (both private and public) and IT sector (both private and public).</p>	Provision in Clause 37 Breach of digital health data	<p>Implementation and operational guidelines shall be provided by the Authority.</p> <p>May be taken up for discussion</p>



## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<p>3. Chapter IV, Point 29(5)</p> <p>This point has a contradiction in itself. The point states "Digital health data, whether identifiable or anonymized, shall not be...." and the explanation given below states "Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance". It is important to note, that in a situation where data is anonymized, the insurance companies would have no way of linking a given health record to that of a particular customer / applicant. Additionally, the ability to share anonymized data is of paramount importance to conducting clinical research and development that helps improve the overall quality of the health system of a nation (and the world at large). In today's era of personalised medicine and artificial intelligence, access to anonymized data can lead to improvement in diagnosis and treatment of diseases such as tuberculosis, brain stroke, cancers etc. Hence, the suggestion here is that this point should only apply to identifiable digital health data and not anonymized data.</p>	Comment addressed in Clause 29 (1)	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding/Remark	Remark
35	USIBC		The U.S.-India Business Council (USIBC) appreciates the opportunity to provide comments on the Digital Information Security in Healthcare Act (DISHA). The privacy and protection of digital health data is a complex and important issue. At stake in this debate are standards that will govern some of the most sensitive data about individuals. It is important that the standards developed today protect individuals in this most personal aspect of their lives, as well as help spur innovation and advancements in medical treatment and technology that will lead to improved outcomes and care. This can be a difficult balance, and it is important this be done right.	NA	May be taken up for discussion
			We also note that discussions regarding a generic data protection law for India, spearheaded by the Justice (Retd.) BN Srikrishna Committee (Committee), are at an advanced stage. (We attach our comments to the experts committee on Data Protection as Appendix A, which include the USIBC submission to the Telecommunications Regulatory Authority of India (TRAI) privacy consultation as well). A perusal of the white paper released by the Committee suggests that concepts such as purpose limitation, data minimisation, storage limitation, etc., are being thought through a consultative process at this stage, however these concepts are already inducted in DISHA. Furthermore, the white paper included personal data in the healthcare and medical context. Therefore, the release of DISHA at this point in time raises questions with regards to the requirement of a parallel full-fledged data protection framework in respect of health-related information, while a broader legislation (which will cut across sectors) is already in the pipeline. We suggest that the Ministry should wait for the outcome of these discussions to consider whether legislation such as DISHA is necessary.	Have provided the comments already provided to Justice BN BN Srikrishna Committee on generic data protection law for India	May be taken up for discussion
			Notwithstanding our concerns about overlap with the broader data protection law, we are grateful for the opportunity to provide our comments on DISHA. However, our group is a trade association made up of approximately 300 members, and we drive to attain consensus on our comments. In order to provide the best advice that reflects the variety of experience, viewpoints, and interests, we respectfully request an extension until May 31, 2018.	Request for extension of time to submit the comments on DISHA	May be taken up for discussion
			Although we would appreciate an extension to enable us to provide a more detailed analysis of the proposal, we have several high level comments to offer at this time. We address these in the attached document along with copies of our privacy submissions to MeitY and TRAI.		

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
36	BSA Alliance		BSA has reinforced this view in its past contributions made to the Government of India in an effort to advance a strong privacy and data protection regime for India's digital ecosystem. For your kind reference, we wish to direct your attention to the following: 1. BSA Personal Data Protection Principles: Our Personal Data Protection Principles seek to guide policymakers around the world towards developing effective regimes for privacy and data protection. The Principles rest on five pillars of data protection: (1) Scope and Definition of Personal Data; (2) Collection, Use, Processing, and Disclosure of Personal Data; (3) Allocation of Obligations and Liability; (4) International Data Transfers; and (5) Personal Data Breach Notifications. A copy of these Principles is attached herewith.	Recommendation for comprehensive data protection framework for India to act as base foundation, upon which sector-specific initiatives can be built.	May be taken up for discussion
			BSA Submission to the White Paper of the Committee of Experts on a Data Protection Framework for India: In July 2017, the Government of India constituted a Committee of Experts to deliberate on a data protection framework for India under the Chairmanship of Justice B.N. Srikrishna ("Expert Committee"). The Expert Committee had released a White Paper in November 2017, seeking detailed inputs from the public on the protection of data in India. BSA contributed to this process, responding to a number of specific issues raised by the White Paper. A copy of BSA's submission to the Committee of Experts on Data Protection is attached herewith.		-
			We share the MoHFW's view that protecting the privacy and security of electronic health data is of utmost importance to India's digital ecosystem, as outlined in the objectives of the DISHA Bill.2. However, there is a need for a consistent and coordinated approach in the formulation of various data protection frameworks. To achieve the objectives outlined in the DISHA Bill, MoHFW should coordinate with other agencies involved in developing frameworks pertaining to data protection, especially the Expert Committee on Data Protection constituted by the Government of India last year. We have elaborated on the need for a consistent and coordinated approach below:		

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<p>(a) <b>There is a need for conceptual consistency across data protection frameworks in India to promote privacy and security:</b></p> <p>The DISHA Bill proposes many concepts pertaining to data protection, such as the types of personally identifiable information, data ownership, consent frameworks, anonymization, security standards, responsibilities of parties, and rights of individuals. These concepts are fundamental to both privacy protection and the data-driven businesses of today, including those of our member companies. Based on our experience working in different jurisdictions, we recommend these core concepts relating to data protection be consistent across sectoral laws and policies at the Central and State level in order to promote privacy and security. It is also important to ensure that data protection regimes are risk-based, recognizing that some data is more sensitive than others, and that this sensitivity is highly context dependent. For example, inconsistent definitions for ‘anonymization’ across laws would create challenges for entities that handle a variety of data types. Conversely, individuals, businesses, and authorities will have a clearer understanding of their rights and obligations in relation to different categories of data if there is conceptual consistency across data protection frameworks. Moreover, any legal, technical, or administrative frameworks that are specifically relevant to the health sector must be harmonized with other laws and regulations pertaining to data protection to promote data privacy and security across the entire digital ecosystem. We understand that the Expert Committee is currently working on developing such a framework, by enumerating specific Data Protection Principles, which would provide conceptual consistency across data protection frameworks in India. We urge the MoHFW to evaluate these principles specifically in the context of the DISHA Bill.</p>		

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<p><b>(b) Consistent obligations across data protection frameworks would promote compliance and help protect individual data privacy:</b></p> <p>The data-driven businesses of today have established systems and processes designed to protect the privacy and security of personal information. Some of these businesses, including BSA member companies, operate simultaneously in different sectors and industries. Generally, the underlying technical architecture designed to ensure data privacy and security is the same or implemented using the same or connected computing infrastructure. We understand that the DISHA Bill empowers the National Electronic Health Authority of India to formulate 'standards, operational guidelines and protocols for the generation, collection, storage, and transmission of digital health data. The DISHA Bill also contemplates other compliance obligations, for example with respect to personal data breaches.</p> <p>BSA advocates that to promote individual data privacy and security such compliance obligations should be risk-based and consistent across sectoral laws and policies at the Central and State level. Consistent obligations would enable service providers to leverage efficiencies of scale and protect individual data privacy. On the other hand, imposing inconsistent or incompatible compliance obligations on service providers would restrict their ability to establish and implement best-in-class technical architecture, which are designed to protect the privacy and security of personal information on a system-wide level.</p>		
			<p>To promote data privacy and security across the entire digital ecosystem, there is a need for a collaborative policy discussion involving all relevant stakeholders:</p> <p>The DISHA Bill seeks to regulate a variety of service providers, such as 'clinical establishments', 'health information exchanges', and other entities that handle 'digital health data'. Given the interconnectedness of information assets and network technologies today, it is important to consider the impact of the DISHA Bill on other stakeholders that constitute India's digital ecosystem such as cloud service providers that enable the collection, storage, and transmission of digital health data. While BSA recognizes the need for regulators to develop regulations that apply to their specific sectors, we believe that a collaborative policy discussion involving all relevant stakeholders is required to achieve the objectives set out in the DISHA Bill. To that extent, we urge the MoHFW to interact with other sectoral regulators, as well the Expert Committee to understand the implications of the DISHA Bill for the larger digital ecosystem in India.</p>		

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<b>Recommendation:</b> BSA recommends that the Government of India coordinate the various policy processes involving data protection across sectors. Specifically, we urge the MoHFW to interact with other sectoral regulators and the Expert Committee to understand the implications of the DISHA Bill for the larger digital ecosystem in India. This will ensure the development of a comprehensive data protection framework for India to act as the base foundation, upon which sector-specific initiatives can be built. Accordingly, it might be prudent for the MoHFW to defer further development and discourse on DISHA till the outcome of the Expert Committee is available.	Recommendation for comprehensive data protection framework for India to act as base foundation, upon which sector-specific initiatives can be built.	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			Currently, DISHA does not sufficiently recognize that the extend of medical data trade as a world-wide phenomenon, a part of what is often referred to as surveillance capitalism. In fact, stunningly, the only two finalists for the Indian Integrated Health Information Platform (IHIP) contract were world's biggest data brokers: IMS Health and United Health (through Optum subsidiary). Both have 100s of millions of anonymized patient data – 500 million for IMS and about 200 million for United Health/Optum, which they sell to other companies. In the draft DISHA anonymization and sharing terms, both will be able to extract and use data:	Concerns expressed in Health data security	May be taken up for discussion
			<p>a. Doctor information is available in the records after DISHA anonymization, and DISHA allows data sharing for insurance claims. IMS has used the first method in the US and elsewhere, to supply data to pharma companies for targeted marketing of medical drugs to doctors and monitoring of their future prescriptions – something that is antithetical to public interest. Optum built its data portfolio from insurance claims of United Health's insurance customers. Insurance companies can set premium based on such data. Other applications such as "health rating" (akin to credit rating) are also being advanced in countries like US.</p> <p>b. The only protection DISHA might have against such data extraction and proprietary use is the clause that data should not be used for commercial purposes. However, we request that DISHA explicitly acknowledges such data trade and uses and will have measures to prohibit them. These include:</p> <ul style="list-style-type: none"> <li>i. DISHA should add data brokers and data companies to the list of companies' data should not be shared with (in 29.5)</li> <li>ii. It should explicitly ban the use of digital health data collected to set insurance premiums or coverage, or targeted marketing, building brand loyalty etc.</li> <li>iii. It should explicitly mention that doctor information need not be shared in anonymized data, unless it is absolutely required. Similarly, for claims data for insurance.</li> </ul>	Concerns expressed in Health data security and allowing for insurance claim and reference to incidences of data broking internationally.	May be taken up for discussion
			3) Right to be forgotten: DISHA, while allows withdrawal of consent, does not allow data deletion on patient demand. Recent laws like the European GDPR allow this. DISHA should also do the same.	Suggestion for allowing Right to be forgotten on patient demand	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			<p>4) Commercial use: DISHA bans commercial use of data but makes it available for various uses such as health and clinical research, academic research, among other things. The problem is that much of these activities are commercial in the real world, run by commercial companies. Hence it is contradictory.</p> <p>For example, EHR data has enormous uses in supplementing clinical trials (which usually is highly commercially run, involving several billions of dollars), since the FDA is now going to use them as Real-World Evidence. Academic research also has interest in patents and licensing and is often funded by commercial companies, or startups by the researcher themselves.</p> <p>DISHA should resolve this contradiction, by explicitly recognizing that such uses are commercial and providing measures to regulate them ensuring citizen and public interest. It may be interesting to note that the health sub-committee of the National Knowledge Commission in 2009 had recommended that:</p> <p>The revenue generated from the commercial use of EHR database should be used for strengthening the health care establishments ... The NHIA (now NEHA) should also hold a share on patent rights of innovations in pharmaceutical and genomic research carried out with EHR database</p> <p>Such measures might have the potential to counter-balance privatization of data's fruits by</p>	<p>Suggestion for providing measures and regulating the commercial interest while ensuring the citizen and public interest</p>	<p>May be taken up for discussion</p>
			<p>Personal information list incomplete: DISHA's list of personally identifiable information is, sadly, incomplete. Please see the figure attached and kindly take measures to ensure that it is at least at the same level as HIPAA. Moreover, DNA, RNA etc. contain considerable identifiable information, and DISHA should account for that.</p>	<p>Suggestion for redrafting of Personal identifiable information list in Schedule 1</p>	<p>May be taken up for discussion</p>
			<p>Re-identification risks: DISHA should recognize that de-identification and anonymization still has the risk of re-identification, especially when coupled with information from other sources ubiquitous in a data rich world. It is said that it takes only 33 bits of information to identify a person out of 6 billion people in the world, and just the information of that he/she lives in a town of one lakh provides half that required information. DISHA should criminalize re-identification attempts and limit the sharing of de-identified data much more (as opposed to anonymized data).</p>	<p>Suggestion for securing digital health data by provisioning for Re-identification risks involved.</p>	<p>May be taken up for discussion</p>



S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
37	Citizen HealthFirst		<p>Recent data linkings:</p> <p>a. Most eHealth programs in the country are based on Aadhaar as a unique ID (IHIP, Kerala, etc.), and often using its OTP/biometrics methods as authentication (e.g., Kerala). DISHA has no entry to regulate it. For instance, what information can be shared with UIDAI?</p> <p>b. Various states (e.g., Kerala) have already linked their eHealth platforms with other state databases, without anonymization, and with the risk of identification/re-identification (see figure). This obviously goes against the spirit of DISHA. Kindly take measures to ensure that such things are prohibited.</p> <p>c. Various other agencies and companies in other countries like US have a practice of linking EHR data with other personal information, such as credit rating and social media information. DISHA should ban such actions.</p>	Concerns expressed in the citizen health data already linked with other state databases without data security measures proposed in the draft Act.	May be taken up for discussion
			Security and privacy compliance: providers and health exchanges should be mandated to provide compliance documents regarding how various provisions of DISHA and other standards such as EHR standards have been achieved by them. Moreover, there should be provision of audit regarding the same, perhaps random audit by NEHA itself.	Suggestion for security compliance by healthcare providers, HIE.	May be taken up for discussion
			<p>Material and human capacity: The FBI in US had issued the following warning: Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.</p> <p>The deadline to transition to EHR is January 2015 (in the U.S.), which will create an influx of new EHR coupled with more medical devices being connected to the Internet, generating a rich new environment for cyber criminals to exploit... the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.</p>	Concerns expressed in data security referring to international developments	May be taken up for discussion
			<p>While we welcome the various privacy and security provisions of DISHA, their proper implementation, apart from legal threat regarding breaches, also needs material help to achieve security. This is especially true in our country of extreme inequality and highly variable capacity.</p> <p>NEHA can issue a security and privacy checklist, provide guidance regarding IT, software, encryption technologies, known vulnerabilities, etc. It can also raise human capacity, in terms of making competent technical knowledge freely available and by increasing sensitization to the importance of privacy and security. This is especially important because the inequality between providers are obvious, and their implementations will likely be.</p> <p>While we understand that it is beyond the mandate for DISHA/NEHA to provide them fully, DISHA should at least provide a clause that NEHA should be able to help any needy local provider across the country with a minimum level of generally usable material regarding these, including free, open source software. In addition to increasing capacity and security, this will prevent wastage and duplication. NEHA should also provide privacy and security training material, including videos, in local languages.</p>	Suggestion for NEHA on enabling privacy and security compliance	May be taken up for discussion

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
			10) Social networks, Apps, mHealth, wearables, IoT: It is unclear to what extent DISHA covers these, since currently it mostly deals with HIEs and providers (just as the US HIPAA is insufficient to cover these modern developments and hence they are currently unregulated). It will be best if it can be made explicit. After all, it is said that "In 10 years, Google street view cars may not only sample images and Wi-Fi networks, but also (DNA, RNA) sequence everything in their paths and pump in real time that information into big data clouds (and link them to their user IDs and other information if they are human)". DISHA should be able to cover such long-term scenarios.	Suggestion for the proposed act to withstand the developments in information science, AI and applications	May be taken up for discussion
			11) Legal access: DISHA says "No Court shall take cognizance of any offence punishable under this Act or any rules or regulations made thereunder, save on complaint made by the Central Government, State Government, the National Electronic Health Authority of India, State Electronic Health Authority, or a person affected.", "For any breach of digital health data by a clinical establishment or any entity an aggrieved person or owner may complain to the State Adjudicatory Authority in writing" That is, out of the various entities that can approach court, only one is a non-state entity, the person affected. Even healthcare providers are not covered, let alone other organizations. This list has to be extended to include the other entities involved. Such a limited list obviously has problems in India, with mass illiteracy, poverty and poor human capacity, especially regarding sophisticated topics such as data trade, breaches and dark net. Thus, DISHA should have provision to ensure that other concerned citizens should also be able to approach court/NEHA regarding breaches, e.g., a mass breach concerning a large number of citizens. Case in point: recently it was reported that the Kerala eHealth database was hacked, and 1 crore citizen records were breached. Yet, the citizen concern regarding it is low, due to poor information and knowledge, and the scattered nature of people. Only other stakeholders, will be able to provide a voice to the people who are impacted. They should be allowed to approach NEHA/court.	Concern expressed in offense punishable under this Act and limitation to save on complaint to cover specific entities.  May be discussed	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
38			<p>a) please clarify if ' other entities" which may have collected data also need to provide view/ modify consent and data to data subject.</p> <p>b) annual audit of data / data flow by external auditor.</p> <p>c) responsibility of data security of sensitive data to rest on a suitably qualified officer in every organization.</p>	<p>a) Addressed in Chapter V</p> <p>b) Provisioned in Caluse 22</p>	May be taken up for discussion

## 909695/2018/E-GOVERNANCE

S.No	Organisation / Institution	Draft Act Clause No	Comment	Finding	Remark
39			<p>It is our firm belief that “Data Protection” requires a comprehensive regulation for multiple sectors and there has to be an “Umbrella Law” that is supported by “Sectoral Security Standards”. ITA 2000/8 already has the concept of “Reasonable Security Practice” with flexibility for sectoral regulators to define their own standards.</p> <p>It is therefore redundant to have multiple Data Protection Legislations leading to multiple Data Protection Authorities, Officers, Committees, Chairpersons etc. Such sectoral laws will be unproductive and create conflicts.</p>	Concern expressed in redundancy with IT Act 200/8	May be taken up for discussion
			<p>we need to consider is whether “Medical Data” is also “Data” which is already addressed by the ITA 2000/8 and Data Protection Act (Srikrishna panel) and whether we can merge these proposed legislations into one existing legislation which should ideally be the “Information Technology Act 2000 as amended in 2008 and to be further amended in 2018”.</p> <p><b>We can then have one State level Adjudication Authority, One Central Level Adjudication Authority for Data in general and one Data Protection Authority supported by sectoral standard committees and sectoral CERTs.</b></p> <p>If this basic concept is accepted, we may have to re work on DISHA 2018 and substitute it with one chapter on Health Data Security in ITA 2000/8 (with some changes in Adjudication and Appellate Tribunal aspects of ITA 2008 which could be as suggested under DISHA 2018).</p>	<p>reference to ITA 2000/8 and Data Protection Act (Srikrishna panel) and merger with the proposed DISHA.</p> <p>Suggestion provided for Sectoral committees and sectoral CERTs to support one Data protection Authority</p>	May be taken up for discussion

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
40	<a href="#">IBM</a>	General	<p>Thanks for giving us a chance to participate in the consultation on Digital Information Security in Healthcare Act (DISHA).</p> <p>Since Health is a state subject under our Constitution, we are sure the Government would take efforts to ensure the passage of the Bill in accordance with the available options.</p> <p>As you are aware, <b>a consultation on the Data Protection Framework and Legislation has just been completed</b>, and IBM actively participated in the consultation process. We would assume you would align <b>DISHA with the Data Protection Framework and Legislation and DISHA bill would be put into process only after contours of the Framework are known</b>. We would be glad to meet you and explain the IBM comments on the Bill, which is set out in the attached document.</p>	Align DISHA with the Data Protection Framework and Legislation	<b>The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.</b>
		Section 3	<p>We express initial concern regarding the definition of “Anonymization” and “De-identification,” as the act fails to address and/or differentiate, in any meaningful way, the specific rules, regulations or actions regarding the lawful and un-lawful use of “anonymized” data v. “de-identified data.” We <b>recommend the Ministry provide additional clarity regarding this distinction</b>.</p> <p>In addition, we also share concern with the Ministry’s <b>definition of “De-identification.” Specifically, we believe the current definition is misguided when it calls for companies to remove all personally identifiable information and "eliminate" the risk of re-identification</b>. We believe a more proven and beneficial approach would align with the pseudonymization standard set forth under the European General Data Protection Regulation (“GDPR”). We <b>recommend the Ministry establish the standard of "very low" risk of re-identification that assesses the risk of re-identification of the data subjects and allows for more robust data for the purposes of public health and actionable insights that can ultimately benefit India’s population</b>.</p> <p>We provide the following amended definition for consideration by the Ministry: “<i>De-identification’ means the process of removing, obscuring, redacting or delinking personally identifiable information from an individual’s digital health data in a manner that makes the risk of unintended disclosure of the identity of the owner very low.</i>”</p> <p>To determine the risk of re-identification, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.”</p>	<p>1)definition of “Anonymization” and “De-identification,” as the act fails to address and/or differentiate, in any meaningful way.</p> <p>2) It may misguided when it calls for companies to remove all personally identifiable information and "eliminate" the risk of re-identification</p> <p>Suggested the amended definition for de-identification</p>	Area of discussion

		<p><b>Section 29(1) - Direct Care and Public Health Activities</b></p> <p>We are concerned with the <b>current approach regarding the use of digital health data between direct care (sections “a-c”) and public health (sections “d-h”).</b> We <i>recommend the Ministry consider the unintended consequences of restricting the use of personally identifiable information solely for direct patient care when precision population health and quality improvement initiatives using personally identifiable information have been shown through myriad examples to greatly benefit the patient population and improve the results of direct patient care</i> .</p> <p>More specifically, such an overly restrictive approach would likely <b>curb scientific research and thereby hinder the rate of development of groundbreaking therapies and cures</b>. Even further, such a requirement could also <b>stifle the ability for India’s clinical establishments to leverage emerging technologies such as data analytics and artificial intelligence to better identify, predict and treat disease using digital health data through individual and population-health precision medicine</b>.</p> <p>Ultimately, the <i>inability for innovators to leverage digital health data at a population level would stifle scientific breakthroughs and yield negative consequences for the health of India’s patient base and the growing healthcare system</i>. This is particularly significant given the growing disease burden facing the country, which according to recent projections, estimate that by 2030 over 100 million people will be living with diabetes with additional one million new cancer diagnosis annually</p> <p>In order to ensure the digital health data can be most effectively used to address India’s disease burden, we recommend the Ministry permit the use of identifiable information for public health purposes (listed as sections “d-h”).</p>	<p>Restrictive approach under this section would likely curb <b>scientific research and thereby hinder the rate of development of groundbreaking therapies and cures</b> and suggested to permit the use of identifiable information for public health purposes (listed as sections “d-h”).</p>	<p><b>Technical Issue</b></p> <p>We may consult the legal expert group and Health Expert and Authority may be consider later</p>
		<p><b>Section 29(5) - Commercial Purposes</b></p> <p>As stated in the above response to “<b>Section 29(1) – Transmission,</b>” we <b>recommend the Ministry consider the unintended consequences of this provision for the health of India’s citizens and the ability for India’s evolving healthcare system to address the growing disease burden. Rather than create additional barriers related to the use of digital health data by restricting use for both identifiable or anonymized data, we urge the Ministry to align Section 29(5) with statutes from countries with forward looking, digitized healthcare systems that understand the benefits and low-risk associated with the use of anonymized and de-identified data for commercial purposes.</b></p> <p><b>For example, in the U.S., Europe, and Japan, once data is anonymized or de-identified it becomes available for use for commercial purpose and falls outside the existing scope of law.</b> To this end, <i>we recommend the Ministry adopt a less restrictive approach in this provision and only limit the use of identifiable digital health data for commercial purposes given the sensitivities associated with inappropriate exchange and use</i> . In turn, all anonymized and Deidentified data would fall outside the scope this law.</p> <p>We provide the following amended definition for consideration by the Ministry:</p> <p><b>“Digital health data, in identifiable form shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government. However, Digital Health data in anonymized and De-identified form may be used for such purposes.”</b></p>	<p>Suggesting the modification in Section29 (5) as:</p> <p>"Digital health data, in identifiable form shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government. However, Digital Health data in anonymized and De-identified form may be used for such purposes."</p>	<p>May be taken up for discussion</p>

## 909695/2018/E-GOVERNANCE

		<p><b>Section 44(1) -</b> We recommend the <b>Ministry consider the unintended consequences of such language that creates a liability standard where an individual and their respective company have the preponderance of the evidence in showing lack of the intention or knowledge of wrongdoing in regard to a violation.</b> As stated, <i>such a liability standard would undoubtedly deter many healthcare innovators from entering India's market given the high level of risk and make it exceedingly more difficult to leverage health information technology to improve health and healthcare.</i></p> <p>While we <b>appreciate the inclusion of a supplemental clause that removes liability if the company or individual shows no knowledge of the actions,</b> we recommend the Ministry <b>amend the proposed standard to presume innocence until proven otherwise.</b> This will spur innovation and ongoing investment in India's healthcare market that will fully leverage health IT investments to reduce India's disease burden and modernize the country's evolving healthcare system.</p>	<p>Suggesting inclusion of a supplemental clause that removes liability if the company or individual shows no knowledge of the actions, and amend the proposed standard to presume innocence until proven otherwise.</p>	<p>May be taken up for discussion</p>
--	--	--	--	---------------------------------------

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
41	<a href="#">Pravagad</a>	Clause No 19, Sub section 2 )	1) Clause No 19, Sub section 2 ) : "No entity shall function as a Health Information Exchange unless <b>established</b> as such by the central Government" - We might go on to say that "No entity shall function as a Health Information Exchange unless <b>authorized</b> as such by the central Government ". But to have it "established" only by the central government may be stretching it too far and will not be the most efficient way of setting up a HIE.	1) Clause No 19, Sub section 2 )- suggested to replace " <b>established</b> " with " <b>authorized</b> " for setting up a efficient HIE	May be taken for discussion
		Clause No 23, sub section 1)  Clause No 35	2) Clause No 23, sub section 1): " To carry out all or any of the powers and functions enumerated in Section 22, the National Electronic Health Authority or its representative, shall have the right to inspect all such records; or access the premises, including virtual premises of the health information exchange or exchanges at any time " - there is possibility of <b>misuse of such an authority. Hence, this should be carefully worded and such powers to access or inspect personal health information should be granted with strong guidelines. While authorities must have full access and ability to audit the processes and methodology of record collection, storage, transmission and use of digital health data, access to personal records must be granted for specific pre-defined purposes. In absence of such a provision this Clause conflicts with Clause No 35</b>	2) Clause No 23, sub section 1): possibility of misuse of such an authority. Strong guidelines should be drafted and <b>in absence of such a provision this Clause conflicts with Clause No 35</b>	Implementation issue  This is an Act and necessary guideline may be developed by the Authority <b>May be taken for discussion</b>
		Clause No 29, sub section 1) and sub section 3)	3) Clause No 29, sub section 1) and sub section 3) : "Digital health data shall not be used for any other purpose, except in accordance with the provisions of this Act. Provided that the digital health data shall be used only for such purposes for which the owner has given consent, or there is a statutory or legal requirement to use the information. " - <b>There is a greater utility for such data, when anonymised as mentioned in Sub section (1) of Clause No 29. Such data can be utilized for big data analytics, training machine learning algorithms and for providing aggregated health insights for the nation or its parts at large. Hence, there must be a clear provision to allow usage of digital health data when "anonymised" or "de-identified". Hence, there is reason to elaborate such use cases with specific guidelines.</b>	3) Clause No 29, sub section 1) and sub section 3) : there must be a clear provision to allow usage of digital health data when "anonymised" or "de-identified"	<b>Implementation issue</b>  This is an Act and necessary guidelines may be developed by the Authority



Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
42	<a href="#">Zoho Corp</a>	Chapter I, 3(m) Chapter II, 15	<b>Chapter I, 3(m)</b> - Relatives should include <b>Son or daughter before brother or sister</b> <b>Chapter II, 15</b> - Meeting is preferred to be on prescribed schedule and made available for public	Suggestion : -Addition of Son or daughter under 3(m) <b>-Fix Meeting schedule</b>	May add Son or daughter under 3(m)
		<b>Chapter II, 19, 20</b>	<b>Chapter II, 19, 20</b> - It is preferred that <b>there are not too many of these Health Information Exchanges</b> . It should be <b>at max one per state. Better to have it region based.</b>	HIE should be region wise	System Specific issue
		<b>Chapter IV, 28</b>	<b>Chapter IV, 28</b> - In the interest of Public health, it is better to store the health information in digital form. <b>(3), (4) refusal clause are not in the public interest.</b> If there is epidemic or so this health information will be useful for taking necessary actions.	<b>Refusal Clause</b>	Implementation issue as there may be a chance of inconsistency between the owner's right with that of collecting Health information in public interest. <b>May be taken for discussion</b>
		<b>Chapter IV, 29 (5)</b>	<b>Chapter IV, 29 (5)</b> - If the owner refuses to give treatment data to Insurance, <b>how will they settle the claim? Need to be suitably modified.</b> I agree that Insurance company should not ask for data to issue new policy.	Claim Settlement in case of refusal of data sharing by owner	<b>Implementation issue</b> <b>Necessary guideline may be developed by the Authority</b>
		<b>Chapter IV, 40 -</b>	<b>Chapter IV, 40</b> - The <b>penalty is too small.</b> It should act as a deterrent. In case of a breach it is responsibility of the HIE which is storing data or the entity using the data to inform the owner.	Penalty clause	authority may take decision later after due assessment

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
43	<a href="#">UL India</a>	CHAPTER III - POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES Part 22 (1)(a)	<b>Part 22 (1)(a): Recognize international and national consensus standards, formulate standards where appropriate,</b> and develop operational guidelines and protocols for the generation, collection, storage and transmission of the digital health data for the purposes of this Act, applicable to	Suggested for considering international and national consensus	System specific suggestion, the act covers entire health sector under Section 22 (1) a However, Necessary guideline may be developed by the Authority
		CHAPTER III - POWERS AND FUNCTIONS OF THE NATIONAL AND STATE AUTHORITIES Part 22 (1)(f):	<b>Part 22 (1)(f): Collaborate and work with national and international standards development organizations, testing, and certification organizations to establish necessary norms and institutions to ensure the quality, security, and interoperability the digital healthcare system.</b>  <b>Proposed new section under Part 22 (1)(f): Collaborate and work with national and international testing and certification organizations to develop a third-party product conformity assessment scheme for health information technology based on the principles of the International Standards Organization (ISO) and International Electrotechnical Commission (IEC) framework</b>	Suggested for considering Collaborate and work with national and international standards	System specific suggestion, the act covers entire health sector under Section 22 (1) f However, Necessary guideline may be developed by the Authority
		SECTION: 28. THE RIGHTS OF THE OWNER OF DIGITAL HEALTH DATA (6)	<b>For Reference:</b> <b>- ASTM E2147-01(2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information systems</b> a) <b>This specification is for the development and implementation of security audit/disclosure logs for health information.</b> It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and <b>includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems.</b> b) The second purpose of this specification is <b>to identify principles for establishing a permanent record of disclosure of health information to external users and the data to be recorded in maintaining it.</b> Security management of health information requires a comprehensive framework that incorporates mandates and criteria for disclosing patient health information found in federal and state laws, rules and regulations and ethical statements of professional conduct. Accountability for such a framework should be established through a set of standard principles that are applicable to all health care settings and health information systems <b>- HIPPA Privacy Rule</b> <b>Permitted Uses and Disclosures.</b> A covered entity is permitted, but not required, to use and <b>disclose protected health information, without an individual's authorization, for the following purposes or situations:</b> (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.18 Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.	Suggestion are based on comparisn with US Fedral standards, healthcare regulations and HIPPA. <b>These are not recommendatory from Underwriters Laboratories[UL]</b> to the Ministry or any other relevant stakeholders in India,	The recommendtaion for removal of clauses under various sections are not justified,  <b>may be taken for discussion</b>

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		<b>CLAUSE: 32. STORING OF DIGITAL HEALTH DATA , SubSection 1 &amp;2</b>	<p><b>with Reference</b></p> <p><b>-Federal Information Processing Standard (FIPS) 140-2 - Security Level 1</b> This standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems</p> <p><b>-Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014</b> Annex A provides a list of the approved security functions applicable to FIPS 140-2. The categories include transitions, symmetric key encryption and decryption, digital signatures, message authentication and hashing.</p>	These are not recommendatory from Underwriters Laboratories[UL]	
		<b>CLAUSE: 33. TRANSMISSION OF DATA Sub section 2</b>	<p><b>with Reference</b></p> <p><b>-Applicability Statement for Secure Health Transport Version 1.2, 3 August 2015</b> This document describes the following REQUIRED capabilities of a Security/Trust Agent (STA), which is a Message Transfer Agent, Message Submission Agent or Message User Agent supporting security and trust for a transaction conforming to this specification:</p> <ul style="list-style-type: none"> <li>· Use of Domain Names, Addresses, and Associated Certificates</li> <li>· Signed and encrypted Internet Message Format documents</li> <li>· Message Disposition Notification</li> <li>· Trust Verification</li> <li>· Certificate Discovery Through the DNS and LDAP</li> </ul> <p>The scope of this specification is limited to the STA features that claim conformance to this applicability statement.</p> <p><b>For Reference:</b></p> <p><b>-Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014:</b> Annex A provides a list of the approved security functions applicable to FIPS 140-2. The categories include transitions, symmetric key encryption and decryption, digital signatures, message authentication and hashing.</p> <p><b>-FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)</b> This standard specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated</p>	These are not recommendatory from Underwriters Laboratories[UL]	
		<b>CLAUSE: 35. DUTY TO MAINTAIN PRIVACY AND CONFIDENTIALITY OF DIGITAL HEALTH DATA SubSection 1,2 &amp;3</b>	<p><b>with Reference</b></p> <p><b>HIPAA Security Rule</b> The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.</p>	These are not recommendatory from Underwriters Laboratories[UL]	

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		<b>CLAUSE: 36.</b> PROCEDURE FOR RECTIFICATION OF DIGITAL HEALTH DATA <b>SubSection 1 &amp;2</b>	<b>With Reference</b> HIPAA Privacy Rule at 45 CFR § 164.526 (a) Standard: Right to amend. (b) Implementation specifications: Requests for amendment and timely action (c) Implementation specifications: Accepting the amendment. (d) Implementation specifications: Denying the amendment. (e) Implementation specification: Actions on notices of amendment. (f) Implementation specification: Documentation	These are not recommendatory from Underwriters Laboratories[UL]	
		<b>CLAUSE: 40. PENALTY FOR FAILURE TO FURNISH INFORMATION, RETURN OR FAILURE TO OBSERVE RULES AND DIRECTIONS, ETC.,</b> <b>SubSection 1 &amp;2</b>	<b>with Reference</b> <b>Breach Notification Rule</b> The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.	These are not recommendatory from Underwriters Laboratories[UL]	

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
44	<a href="#">Asia Cloud Computing Association (ACCA)</a>	Chapter I: Section 3.1.j (Definitions)	The ACCA <b>seeks clarity on the term "data owner"</b> , which by the above definition refers to a data subject, i.e. the person whose digital data is being processed. We thus interpret that as per the draft Act, the <b>role of the "Chief Health Information Executive" will be that of "data controller"</b> . Data protection laws allocate responsibilities in regard to how a party interacts with data, and the level of access and control they have over that data. One approach, common to many international standards and the regulations in many jurisdictions, <b>is to distinguish between a data controller, data processor and data subject</b> . The concept of control of the data focuses on whether the data user can exercise stewardship over the data, be confident that the data is up-to-date, and to access or recover that data in the event that the primary data repository is not available for any reason.	definition of <b>"data owner" be in line with India's broader Data Protection Framework</b> – which is currently in consultation-, in order to maintain consistency in terminology across India.	System specific and implementation issue  However, Necessary guideline may be developed by the Authority
		Section 21 (The Chief Health Information Executive and his functions), Section 32 (Storing of digital health data), Section 37 (Breach of digital health data), Section 38 (Serious breach of digital health data)	<b>seeks further clarity on what constitutes "appropriate measures"</b> when referring to adoption of cybersecurity solutions in <b>Section 21.2.c</b> . The ACCA notes MoHFW's efforts to protect personal information as evident from the Act's <b>data breach</b> notification requirement laid out in <b>Section 21.2.d</b> and the explanation of breach v.s. serious breach detailed in <b>Sections 37 and 38</b> . We recognise that requiring data breach notifications may <b>create a situation of "notification fatigue"</b> , which may have the unintended consequence of individuals or organisations failing to take the necessary steps to protect themselves as data breach situations requires resources to carry out careful assessments ascertaining the facts and causes of the breach, in order to decide the necessary and appropriate action. The ACCA makes the following recommendations on <b>data breach notification</b> : (i) <b>Adopt a harm-based approach</b> with regard to notification to individuals, i.e. that notification to individuals and the data controller should only be required when the data breach reaches the threshold of actual serious and material harm to individuals or organisations. This approach has been adopted in other countries, such as the data breach guidelines issued by the Japanese Data Protection Authority. (ii) <b>A single notification timeframe should be put in place</b> within the India Digital Information Security in Healthcare Act, and in line with the draft Data Protection Framework, which will be applicable to all notifications made to affected individuals and the data controller. Uniformity across the proposed Act will provide clarity for organisations and increase compliance. This is preferable to multiple timeframes which results in ambiguity and an impact on resources for organisations. In this respect, ACCA recommends that the timeframe for notification be "as soon as practicable and without undue delay". Having a single timeframe is preferable, rather than requiring notification within a specific number of hours. (iii) <b>If a notice obligation that references a specific number of hours is to be prescribed</b> , it should be clear that the obligation is only: a) applicable to the organisation that originally collected the personal data (as compared to a service provider or data intermediary of that collecting organization); and b) triggered when that entity has actual knowledge of the breach.  The ACCA requests further clarification on the <b>"prescribed mode" of digital health data storage referenced in Sections 21.2.e and 32</b> . The ACCA commends MoHFW's acknowledgement of the benefit of sharing patient data between hospitals as laid out in <b>Schedule I section on Personally Identifiable Information</b> . Further data sharing between economies through cloud computing can enable a firm to leverage global economies of scale for cost-savings. <b>Data localisation measures may not necessarily boost data protection</b> and data is not necessarily safer because it resides within a particular jurisdiction, rather, an institution's level of security and ability to protect data is determined by its technical know-how. <b>Data localisation laws mean that firms face unnecessary limitations when looking for technological solutions, often creating an artificial barrier to economic benefits.</b>	India work to ensure its policies – including the <b>DISHA – supports digital trade through allowing cross-border flow of data.</b>	Breach identified later may be addressed in the act or should be defined by the authority. However, Necessary security guideline may be developed by the Authority
		Section 22 (Powers and functions of National Electronic Health Authority of India) and Section 23 (National Authority's power of oversight, inspection, investigation and issuance of directions etc.)	The ACCA takes note of MoHFW's initiative to establish a statutory body in the form of the National Electronic Health Authority of India, to enforce privacy measures and regulate the storage and exchange of digital health records. We take the view that <b>an independent regulatory body is well-positioned to regulate policy in a fair and prudential manner</b> . Further, <b>a specialised regulator will have better opportunities to coordinate internationally with other similar agencies</b> , as well as react appropriately to specific consumer and business concerns surrounding the regulation of data. In this regard, the ACCA recommends <b>following international standards when determining the powers and functions of the National Electronic Health Authority of India</b> . We do, however, note that <b>setting up a new digital health authority may generate additional costs associated with building a new entity</b> . The ACCA thus encourages MoHFW to be open to comment and be flexible during the establishment of such an authority and consider <b>allowing third party certified/qualified auditors to access and assess records</b> .  The ACCA seeks <b>clarity on the structure and establishment of Health Information Exchanges referred to in Section 19</b> . The ACCA also requests <b>further information on the nature of "virtual premises"</b> of the health information exchanges mentioned in Section 23.1 in relation to the data access rights of the National Electronic Health Authority.	Suggested to set up a independent regulatory Body and specialised regulator for international collaboration	The NeHA may take decision later on that according to need and utility
		Section 28 (The rights of the owner of digital health data) and Section 31 (Ownership of digital health data)	The ACCA notes that as per the draft Act, the owner of the digital data will have <b>"the right to require their explicit prior permission for instance of transmission or use of their digital health data in an identifiable form"</b> (Section 28.8.b) and will also have <b>"the right to be notified every time their digital health data is assessed by a clinical establishment within the meaning of Section 34 of the Act"</b> (Section 28.8.c). In this regard, the ACCA highlights that <b>the consent framework should enable the collection and use of data that is suited to the context, and is clear, transparent and reasonable</b> . A flexible approach that allows for notice to be given to the data subject and consent in the context of the use of the data will address future developments in technology.	Suggestion for patient consent framework to be developed	<b>Implementation issue</b>  However, Necessary guideline may be developed by the Authority
		Schedule I (Personally Identifiable Information)	The ACCA commends MoHFW's <b>emphasis on information sharing between hospitals and encourages</b> MoHFW to further expand this to allow data to move between GPs and hospitals within India and between different economies in order to benefit from the cross-border flow of data and enhance the digital infrastructure of medical facilities.  The ACCA encourages MoHFW to ensure that <b>the PII categories laid out in Schedule I of the Act are in line with the international certification standards for privacy</b> .	Suggestion for follow internation guidelines for PII	<b>Implementation issue</b> However, Necessary guideline may be developed by the Authority

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
45	<a href="#">Nishitha Ehealth</a>	NA	Proposing a Application for Ehealth regarding data collection,storage,retrieval.	<p>The application is on the same concept as PHRMS. Ministry has already taken such initiative</p> <p>Comments provided not specific to DISHA</p>	<p>Comments provided not specific to DISHA</p> <p>No action required</p>

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
46	Narayana Health	Chapter II 5 (1) (c)	<b>Composition of the National health authority.</b> It has to include a member from the medical community. <b>Public health professionals are not the same as doctors working in hospitals and they work under very different circumstances with very different data sets.</b> There has to be a representative from the community of healthcare specialists who is a working professional in one of the hospitals that will be working with this data. <b>26 Power of a Civil Court:</b> The rule-maker can't also be judge and jury. This goes against the principle of separation of powers.	Suggestion provided Composition of the National health authority	provision for the same has already provided under clause 13,  However we may taken up for discussion
		Chapter IV 28(3)	<b>Remove the term "withdraw consent".</b> Once a medical record is created, it is very difficult to remove it from the system without affecting all the other fields attached to it. At best, the hospital can remove the identifiers of that patient so that it no longer links to that name. But it's very hard to remove one lab report out of a daily tally of thousands	Expressing the concern in implementation of withdraw consent	Implementation issue, may be discussed
		28 (8) (b)	It will be <b>operationally impossible to get the patient consent for every single time their digital data is transferred around an organization.</b> For example – we have a hospital in Jammu but the lab reports are analysed in Bangalore in large batches. It will affect our turnaround time if we have to get every test individually consented before sending it out for analysis. <b>Change it to a system of 1-time consent.</b>	Suggested one time <b>consent system</b>	Implementation issue, may be discussed
		28 (8) (f)	<b>How can a hospital treat a patient if they don't consent for the hospital to generate patient data?</b> That puts the hospital at risk tomorrow if the patient sues them for incorrect treatment. <b>The hospital won't have a record to prove that everything necessary was done.</b>	Raised concern incase of patient deny to give consent to hospital for Health Data record	Implementation issue, may be discussed
		28 (8) (g)	This will <b>destroy India's underdeveloped health sector. Small nursing homes won't be able to invest in the cybersecurity tools to keep the data safe.</b> They will be destroyed if patients are allowed to claim compensation for data leaks. Damages from leaking medical data rank very low in the list of healthcare priorities for this country. We can only afford to have this when the data environment is mature.	Expressed concern for entities to bear the cost of security compliance	Security and Implementation Issue  May be taken for discussion
		30 (3)	Make this as a <b>digital consent form</b>	Make this as a digital consent form	Standards would be defined by the Authority, paper records are not part of the act as of now and are governed by Medical Council Code of Ethics. May be taken for discussion
		35 (5)	Request this to be changed it to <b>"in case of notice of any breach or..."</b> . Not all breaches are detected and the establishment can at best inform the patient once they themselves know there has been a data breach.	Expressed concern about wording of clause and suggested modification	may be consider
		37 (2)	<b>Request this to be removed. Paying damages will disincentivize the adoption of medical records by smaller medical establishments, clinics, etc.</b>		Area of discussion
		40	<b>Request this to be removed.</b> It will not make clinical establishments happy about adopting digital medical records if their compliance costs go up	Expressed the concern under section 40 highlighted and suggested modification	
		50	<b>The Legality of this clause need to be checked. You can't create a parallel legal system just for the sake of medical records</b>	Mis-interpretation of section	No action required
		Schedule 1 (xi)	<b>To be removed. Physical, physiological and mental health conditions are not Personally identifiable information</b>		

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		Schedule 1 (xiii)	<del>remove this.</del> Medical records are not personally identifiable information. Patient is always referred to by "Patient" or "Subject" – not by his/her name. This clause will hinder the ability of medical students to learn how to treat patients before they have become registered doctors. They have to study patient records and analyse patients without learning their name. If this data is firewalled, medical schools will have to shut down.		
		Item 33 (2)	states that <b>clinical establishment "may" transmit digital health data to health information exchange after retaining a copy for "reasonable" use.</b> This means for any clinical establishment it is "elective" to share digital health data with other parties. That can cause problematic situations of uneven availability of digital health data across the country. In the case of Australia, it is legal mandated that any clinical establishment "must" share digital health data with other parties.		implementation issue
		Item 38 (1) (b) :	<b>This requirement is onerous.</b> It will act as a dis-incentive for clinical establishments to share data with exchanges or other clinical establishments <b>for the fear of committing serious breach of digital health data that contains information that isn't anonymized.</b> Meaning the whole purpose of such digital health data exchange could be mute, if you can't identify the specific citizen whose digital health data is wanted for whatever care purposes. Technology, administrative, process failures always occur, and all organizations know that inspite of proper preparations and efforts to implement. To say you can go to imprisonment because of some unintentional failure of technology, administrative or process associated with anonymous aspects of data seems onerous. The reaction of this point ... clinical establishments won't risk maintaining digital health data for fear of imprisonment. <b>My recommendation is this point should go into Item 37 rather than Item 38.</b>		May be consider if suitable with discussion  Further, Breach identified later may be addressed in the act or should be defined by the auhtority.
		Section 6:	The National Executive Committee should also <b>include a person from the medical community</b>		May be consider if suitable with discussion
		Section 8:	The State Electronic Health Authority should also include <b>a person from the medical community</b>		
		Section 22,23,24	The Government should looks an incentivising the providers for EMR adoption.What will be the Information Security standards that the Central and State Health Authority will comply to? What are the controls that a provider should comply to? <b>Section 23:</b> There has to be a structured mechanism to access the providers premises by the Electronic Health Authority officials. The provider should be clearly briefed on the issue before doing any such activity.	incentivising the providers for EMR adoption.	Implementation issue
		Section 28:	Hospital collects multiple details of the patient and it is not possible to turn over all data. <b>The Information that needs to be shared to the patient (dataset) needs to be defined</b>		General suggestion
		Section 28, 96	How can a patient get to know this information ? This is not clear.	The Government of India already has a repository of all the citizens through the Aadhar system. Is there a plan to tag Aadhar with the patient record?	
		Chapter V:	Liability limits has to be capped.		General suggestion



S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
47	<a href="#">Healthpix</a>	38(d)	<p>This clause in its <b>current form does not make a distinction between commercial usage such as selling of data in its raw form (de-identified or otherwise)</b> and commercialization of analytics of de-identified healthcare Information to create RWE (real-world evidence) and insights that are essential to the future of medicine as depicted below for various Healthcare stakeholders:</p> <p>a) <b>Pharmaceutical R&amp;D:</b> Today, Pharma R&amp;D increasingly depends on Real World Evidence for Drug discovery, measurement of efficacy, optimize trials, quick feedback from real world, spot adverse events for their drugs, education &amp; awareness, etc. In 2016 alone, Pharma has made \$6.5 Billion investments in digital health companies across the globe. RWE is of Top 2/3 priority for Pharma R&amp;D. Since Pharma is prohibited from owning the healthcare data (de-identified or not), they can only depend on Analytics through commercial partnerships.</p> <p>b) <b>IBM Watson &amp; Cancer care AI:</b> IBM Watson isn't a clinical establishment, but a proprietary cognitive compute algorithm used by clinical establishments across the globe including in India. IBM Watson algorithm will be trained by de-identified healthcare information drawn from patient medical records. This helps in recommending the right cancer treatment based on patient persona who now needs the treatment. IBM Watson is a paid service used by doctors &amp; hospitals. If these regulations prohibit commercial gain coming from RWE, then all patients will end up receiving cancer treatment by blindly following a One Size Fits all approach - which is known to be ineffective in a heterogeneous disease such as cancer/chronic diseases.</p> <p>c) <b>Artificial Intelligence (AI) in Healthcare:</b> Entire AI in Healthcare depends on analysis and pattern recognition on the de-identified healthcare information and training the algorithms for each disease and patient persona. Early detection of diseases, Diagnosis, Treatment, Clinical decision support systems and R&amp;D in Healthcare are undergoing transformative changes using AI. And there are many such AI solutions that are commercially available and are used by the medical practitioners to enhance care.</p> <p>d) <b>Clinical Research Organizations (CROs):</b> All CROs today, bridge the gap between Pharma R&amp;D and the real-world data.</p> <p>e) <b>Precision Therapies and Genomics:</b> Is the future of Healthcare, and Precision Therapy solely depends on patient persona and the relevant medication. Without AI, Analytics and RWE, Precision Therapy will not see the light of the day!</p>	<p>Expressing the concern that current form does not make a distinction between <b>commercial usage such as selling of data in its raw form (de-identified or otherwise)</b> and commercialization of analytics of <b>de-identified healthcare</b></p> <p>To Foster innovation, <b>it is imperative for the Govt to make a distinction between Analytics/Real World Evidence (RWE)/AI and the Raw Data in itself, and include provisions for Analytics/RWE/AI under various clauses of DISHA</b> and yet enforce strict rules on the way Creation, Storage, &amp; Transfer of all the 3 aspects of Healthcare Data are done by paying unwavering attention to ensure patient confidentiality and privacy</p> <ul style="list-style-type: none"> <li>- the proposed act does <b>not take cognizance of RWE/Analytics/AI</b>, it could potentially stifle clinical innovation and also enormously reduce FDI investment into Digital Healthcare in India.</li> <li>- suggested inclusion of a definition and specific provisions for <b>“digital health data analytics”</b>; and its commercial use.</li> <li>- Additionally, creation of distinction between requirements for use, storage, transmission of “digital health data” and requirements for use, storage, transmission of anonymized or de-identified “digital health data analytics”.</li> </ul>	May be taken for discussion usage of anonymised/ de-identified data for commercial uses which shall also lies in public interest
		Clinical Establishments, Health Information Exchange, Other Entities:	<p><b>Clinical Establishments, Health Information Exchange, Other Entities:</b></p> <p><b>Preliminary draft underlines that Clinical Establishments are the ones who will typically generate digital data and Health Information Exchanges are the ones where data will predominantly reside.</b> However, we would like to highlight that usage of cloud-based healthcare software is on the rise, many of these clinical establishments use the software to store data on the cloud directly. There isn't an intermediary stage of Transfer in any of such cases. Hence, it is logical for EMRs, Hospital Information Systems, Lab automation software, consumer healthcare devices and other digital tools in healthcare to be included in the definition of Clinical Establishments or make them part of Health Information Exchanges in the context digital health.</p> <p>Please <b>Include EMRs, HIS, Lab Software etc. under Clinical Establishments or under Private Health Information Exchange.</b> These <i>firms should fall under clause 29(1) and not under 29(2) given that these are the firms that are enabling activities listed under 29(1) a to h.</i></p>	<p>suggesting to put up firms like EMR, HIS Lab under Clinical Establishments or under Private Health Information Exchange.</p> <p>Also it should fall under clause 29 (1) not under clause 29(2)</p>	Implementation issue. Authority can take decision later and review the <b>clause no 29 (2)</b>

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
48	<a href="#">XIAOMI Technology</a>	Section 3(1)(c) – Consent	1.The definition should specifically <b>clarify that proxy consent needs to be given by Guardians or Relatives</b> , as the case may be, for individuals who are minors, of unsound mind or are ineligible to contract as per the laws in force should be excluded from the definition of Owner. 2. It is not clear if the <b>onus of ensuring that the „consent“ is given “...after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data”</b> is on the person collecting digital health data. The Act must prescribe some indicative points on what constitutes consent after understanding the nature, purpose and consequences of collecting and dealing with digital health data. 3. The Act is silent on <b>whether „consent“ can be revoked retrospectively by the Owner on grounds of having failed to have understood the nature, purpose and consequence of the collection, use, storage or disclosure and the recourse that collection agencies may have.</b>	Requested more detail clarity on CONSENT	MCI Code of ethic regulation defines the "Consent" and same may be applicable for DISHA act.
		Section 3(1)(d) – "De-identification"	1. <b>“Anonymized” and “de-identified” digital health data should be afforded treatment commensurate with the risks involved in the event of breach of either.</b> 2. Since <b>anonymization</b> is intended to be <b>permanent</b> , while <b>de-identification</b> is <b>temporary</b> and reversible, breaches of anonymized data pose limited threat to the owners, and should have minimal constraints, if any, in terms of collection, transmission, storage, use, disclosure and access. <b>De-identified data, in turn, must have lesser constraints than personally identifiable digital health data, but more than anonymized digital health data.</b> 3. The <b>collection, storage, transmission, use, disclosure and access to personally identifiable digital health data for a specified purpose should be permitted</b> , provided the owner explicitly consents to the same.	Expressed view on the risk involved in disclosure of “Anonymized”/ “de-identified”/ personally identifiable digital health data	No action required However, National authority may consider these suggestion while drafting the guidelines
		Section 3(1)(e) – "Digital Health Data"	The restrictions on collection, storage, transmission, use, disclosure and access should be imposed proportionately depending on whether the digital health data is personally identifiable, de-identified or anonymized. <b>The definition of “digital health data” must accordingly be modified to exclude anonymized data, or both de-identified and anonymized data.</b>	suggesting modification in definition of DHD	No clarity in the comments. However may be taken for discussion
		Section 3(1)(m) – "Relative"	1. <b>Provision for adopted descendants need to be included.</b> 2. The Relatives listed <b>should be eligible to provide „Consent“, as defined under the Act.</b> We suggest the <b>definition of Relative be limited to those relatives who are competent to contract as defined under the Contract Act, 1872.</b>	Suggesting definition of Relative be limited to those relatives who are competent to contract as defined under the Contract Act, 1872	MCI Code of ethic regulation defines the "Consent" and same may be applicable for DISHA act.
		Section 3(1)(o) – „Sensitive health-related information"	1. Sensitive health-related information is currently defined to mean “... <b>information, that if lost, compromised, or disclosed, could result in...</b> ”. 2. In line with the intent, it should be clarified that Sensitive health-related information means <b>“personally identifiable digital health data that if lost, compromised, or disclosed, could result in...”</b> . 3. The definition is highly subjective and terms such as <b>“substantial harm”, “embarrassment”, “inconvenience”, and “unfairness” are undefined and ambiguous.</b>	Requested clarification on Sensitive Health Data definition	May be taken for discussion and National authority may elaborated it later in guidelines
		Section 28(6) – The rights of the Owner of Digital Health Data  Section 28(7) – The rights of the Owner of Digital Health Data	1. It is not clear who is responsible for making this accessible to the owner, and how. 2. Any single entity or clinical establishment will be able to provide information only regarding the clinical establishments or entities to which such entity has transmitted, disclosed or given access to. Information regarding further downstream disclosures, transmissions and <b>access will not be available with the upstream entity.</b> 3. Individual entities and clinical establishments will, therefore, not have aggregated consent, transmission, disclosure and access and consent related information; the obligation should be imposed on health information exchanges.	Expressed view on Accessibility /disclosure/transmission of digital Health Data and also highlight the non availability of access with the upstream entity.	May be taken for discussion and National authority may elaborated it later in guidelines

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		Section 28(8)(b) – The rights of the Owner of Digital Health Data	<p>1. There are <b>multiple parties involved in the collection, storage, processing and transmission of digital health data</b>. Such collection, storage, processing and transmission may be outsourced to third parties who have specific expertise in the particular process as well. Given this, it is <b>practically not feasible to obtain the consent of owners for each instance of transmission</b>.</p> <p>2. The <b>current wording of the clause also implies that consent for transmission or use of digital health data, only if in an identifiable form, will have to be taken on a case to case basis. There should be an enabling provision permitting anonymized or de-identified digital health data to be transmitted or used to any number of parties with a one-time consent for the purpose for which consent was taken.</b></p> <p>3. It is also clear whether explicit prior consent is required only for transmission or use, <b>but not for collection, storage or access</b></p>	Suggestion for One time consent	implementation issue. The authority may consider later
		Section 28(8)(d) – The rights of the Owner of Digital Health Data	<p>1. <b>“Health emergency”</b> must be defined.</p> <p>2. <b>“Family members” should be replaced with “Relatives” or “Guardians”</b> as defined under the Act.</p>		may be consider
		Section 28(8)(e) – The rights of the Owner of Digital Health Data	<p>1. “Sensitive health-related information” is a defined term, but <b>“sensitive health-related data” is not</b>.</p> <p>2. It is <b>not clear on how this right is proposed</b> to be implemented and enforced.</p> <p>3. It is <b>not clear if the owner, at his/her own discretion, determines whether the disclosure of his/her sensitive health related information is “likely to cause damage or distress”</b>.</p> <p>4. <b>“Distress” is an undefined and ambiguous term</b>. The qualification of “that is likely to cause damage or distress to the owner” should be deleted as the definition of “sensitive health related information” suffices.</p>	expressed their concern about Sensitive Health Data	May be taken for discussion
		Section 28(8)(f) – The rights of the Owner of Digital Health Data	<p>1. The provision of several direct and indirect care services is dependent upon the generation and processing of digital health data, and cannot be provided unless such consent is provided. We propose that the right be limited to refusal to consent to storage, transmission and disclosure of identifiable digital health data.</p> <p>2. <b>“Health service” is an undefined and ambiguous term</b>. There must be clarity on what constitutes “health service” along with illustrations.</p> <p>3. Healthcare products like fitness bands, automated weighing scales, diabetes check devices collect “digital health data”. The generation, collection, storage, use, disclosure and transmission of digital health data by such is currently excluded from the purview of the Act.</p>	express their concern about Healthcare products and Health Services	May be taken for discussion
		Section 29(1) – Purpose of collection, storage, transmission and use of the digital health data	<p>1. <b>“Personally identifiable information” should be replaced with “personally identifiable digital health data”</b>.</p> <p>2. It needs to be clarified that <b>de-identified and anonymized data may be used for all purposes under (a) to (h)</b>.</p>		No action required
		Section 29(2) – Purpose of collection, storage, transmission and use of the digital health data	<p>1. In addition to generation, collection and storage, the enabling provision must be extended for access, use and transmission as well.</p> <p>2. <b>Entities must be permitted to generate, collect, store, access, use and transmit anonymized and/or de-identified digital health data for the purposes in clause (d) to (h) of Sub-Section (1) as well.</b></p>	Requested for permission to access, use and transmit anonymized and/or de-identified digital health data for the purposes in clause (d) to (h) of Sub-Section (1) as well.	may be consider in consultation with expert committee

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		Section 29(5) – Purpose of collection, storage, transmission and use of the digital health data	<p>1. This is an <b>ambiguous blanket restriction on use of all categories of digital health data for any “commercial purpose”</b>.</p> <p>2. <b>“Commercial purpose” must be defined.</b></p> <p>3. <b>Use of anonymized digital health data should be permitted for commercial purposes without the requirement of seeking consent on a case to case basis, since there are limited, if any, chances of owners being adversely affected.</b></p> <p>4. <b>For example, several health services and facilities can be advertised and made available using anonymized and/or de-identified digital health data.</b> Creation of awareness of availability of health products, services and facilities should not be stifled since <b>use of anonymized and de-identified data will not pose threats to owners, and is beneficial for customers.</b></p> <p>5. There must not be an outright bar on use of personally identifiable digital health data for commercial purposes. If owners give explicit consent for the access, use, disclosure, storage and transmission of their personally identifiable digital health data for commercial purposes, the same should be permitted as consent of the owner is primary.</p> <p>6. <b>It is not clear whether owners may access, use, disclose or store digital health data, whether</b></p>	<p>Need to Define "Commercial Use"</p> <p>Limit the scope of advancement and research</p>	Mat be taken for discussion
		Section 30(2) – Collection of Health Data	<p>1. Enabling provisions to be extended to entities in addition to “clinical establishments”.</p> <p>2. <b>“Health data” should be replaced with “digital health data”.</b></p> <p>3. Since the transmission of digital health data requires consent of the owner, as provided for under Section 33(3), sub-clauses (c) and (d) of Section 30(2) may be deleted.</p>	Suggesting modifications in definitions under section 30 (2)	Mat be taken for discussion
		Section 30(3) – Collection of Health Data	Illustrative templates of the consent form may please be annexed as schedules to the draft Act.		MCI Code of ethic regulation defines the "Consent" and same may be applicable for DISHA act.
		Section 30(5) & 30(6) – Collection of Health Data	<p>1. Enabling provisions to be extended to entities in addition to “clinical establishments”.</p> <p>2. Circumstances where “proxy consent” may be taken to be limited to where owner is incompetent to contract as per the provisions of the <b>Indian Contract Act, 1872.</b></p> <p>3. Persons from whom “proxy consent” may be taken to be restricted to “Guardians” and “Relatives” as defined under the Act.</p>	Express concern about Consent	
		Section 32 – Storage of data	Enabling <b>provision permitting the storage of digital health data by entities must be incorporated.</b>	Requested for incorporation of permission of storage and access of DHD by entities	May be taken for discussion
		Section 34(2) – Access to digital health data	Enabling <b>provision permitting the accessing of digital health data by entities must be incorporated.</b>		
		Section 34(4) – Access to digital health data	<p>1. Process for providing access to investigating authorities should be dependent upon <b>whether the digital health data requires is personally identifiable, de-identified or anonymized. Permission for access to anonymized digital health data should not require an order from the competent court.</b></p> <p>2. Even where an investigating authority requires access, the consent of the owner should be sought first. <b>If access to personally identifiable data is not consented to by the owner, only then should an order of the court be made necessary.</b></p>	Express the view on access of DHD as Permission for access to anonymized digital health data should not require an order from the competent court	May be taken for discussion
		Section 37(1) – Breach of digital health data	<p>1. <b>“Digital health information” should be replaced with “digital health data”.</b></p> <p>2. All the rights granted under <i>Section 28 to owners are not exercisable uniformly against the concerned stakeholders</i> i.e. NeHA, SeHA, HAs, clinical establishments and entities. The <b>remedy for breach of Section 28 should also explicitly clarify that the remedies are available only against such persons who have an obligation to make the rights under Section 28 available.</b></p>	Need clarity between DHI & DHD and also on <b>remedy for breach under Section 28 however, the provision in this relation already given under Section 37(2)</b>	Section 37 and 28 may review by expert committee
		Section 38 – Serious breach of digital health data	<p>1. <b>“Negligent” breach of digital health data is covered under Section 37, and should not be considered a “serious breach”.</b></p> <p>2. <b>Sub-section (1)(c) is duplicated in Section 37(1)(c).</b> Failure to maintain security standards, unless repeated, <b>should not be considered a “serious breach” and should be deleted.</b></p> <p>3. <b>Sub-section (1)(d) should be deleted since use of anonymized digital health data without consent does not pose any threats to owners.</b> If consent for use of de-identified and personally identifiable data is taken from the owners, then use for commercial purposes or commercial gain should not be considered a breach.</p> <p>4. <b>“Commercial gain” must be defined.</b></p>	<p>Express concern about Negligent” breach and mentioned the Duplication of some sub-sections,</p> <p><b>“Commercial gain” need to be defined.</b></p>	<p>No such duplicacy found in the act.</p> <p>Act clearly distinguish between section 37 (c) and 38(c )</p>

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		Section 44(2) – Offences by companies	Sub-section (2) of Section 44 is a repetition of sub-section (1) and should be deleted.	Specified Duplicacy of section	No action required as the section are self explanatory

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
49	Amarnath DS	NA	<p>I would like to congratulate the honourable ministry and the team to come up with the detailed policy regulation on protecting personal health records. Below are couple of recommendations I have to explicitly add to the document:</p> <p><b>1. Provision to define access to persons health information during an health Emergency.</b> E.G Break the Glass.</p> <p><b>2. Inclusion of an Individual's photograph as part of 'Personally Identifiable Information'.</b> I am not sure biometric covers above.</p>	General Comments	may be taken for dicussion

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding/	Remarks
50	<a href="#">Blume Ventures</a>	subpoint (e)(i) of Section 3	The draft act defines a <b>health record as a Digital Health Data</b> , which is basically any piece of information related to an individual's health condition. <b>It doesn't clearly define the difference between a DHD and other demographic parameters</b> like weight, height, skin type, hair colour etc. We believe the subpoint (e)(i) of Section 3 which states <b>"Information concerning the physical or mental health of the individual"</b> is defined vaguely. Some companies like HealthifyMe use most of the demographic parameters and are generally not concerned with any health condition. <b>Blume's view is that they shouldn't have to fall in the purview of DISHA.</b>	Suggest modification in the general terms like Demographic detail, Usages of EHR, penalty, Commercial usage of data which Legal expert of MoHFW have already discussed in detail during drafting of action	No action required  MDDS
		subpoint (c)(i) of Section 3	As the law is defined currently, <b>clear consent is required to be taken for each instance of usage of health records by a service provider.</b> In practice, companies which deal with a series of data may find it hard to take consent each time even though the usage of the data has not changed. We think it is best if the protocol is <b>modified to take a one-time consent on a particular device and is stored either permanently or renewed once every six months or so.</b>	<b>Suggesting one time consent</b>	may taken for discussion
		Clause (g) in Section 28	<b>LIABILITY OF THE DIRECTORS IN CASE OF A BREACH OF HEALTH INFORMATION AND MATTERS RELATED TO COMPENSATION</b> states that the owner of the health data can claim compensation for breach of the digital health data. Blume's view is that <b>despite the best efforts, systems and policies by the founder of companies, in several cases it has been observed that individual employees are involved in events of data theft.</b> Such cases have been frequently observed in financial services and real-estate industries. It is imperative that <b>clear-cut guidelines will be arrived at by NEHA (and SEHAs) to ensure that there's no undue harassment by the aggrieved owners towards creators and transmitters of digital health data.</b> Part of this relief <b>could be limiting the maximum liability on the part of the company to a fixed amount, say Rupees One Crore,</b> such that companies can take requisite insurance to cover this risk. Further, even in cases of serious breach of health data (which in some cases could be directly attributable to one or more employees of a company), our view is that the imposition of <b>criminal penalties on Directors is too harsh a provision.</b> The matters <b>should be rightly referred to the right adjudicating authorities for proper hearing before assigning any criminal penalty.</b>	<b>Express the view on compansation</b>	National authority may draft the guidelines for compansation for damage/loss and also put the provision for forming investigating committee
		Section 29	<b>THE ISSUE OF BUILDING DERIVATIVE PRODUCTS AND SERVICES</b> <b>Tricog's algorithm</b> Tricog is involved in the business of giving ECG analysis as a service. They are creating an algorithm using the health data that it owns as part of its contract with the clinics and hospitals in its network. It is expected that clinics and hospitals will have a back-to-back agreement with the patients who are the eventual beneficiaries of the Tricog service. In creating this algorithm, as long as only anonymised data is being used, <b>an important question, of who owns the benefits of it, arises.</b> As and when Tricog will make this algorithm available on an API to its customers (who could be Pharma or medical device companies in some cases), this could be construed as <b>"commercial usage" of the health data.</b> This is <b>something that is expressly prohibited in Section 29 of this draft act.</b> Blume view is that <b>any development of such algorithm that stands to benefit the society as a whole, despite being built as a part of a for-profit company, should be allowed under the proposed law.</b> Our view is that while owners have right on their digital health data, any product that is created out of wholly anonymised or de-identified data should be allowed to exist in commercial domain. This is the best way <b>to allow innovation to take place, balancing the concerns of privacy.</b>	<b>Express the view on comercial usage of data</b>	may taken for discussion

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding/	Remarks
		Section 29 (5)	<p>BeatO's aggregated health rating</p> <p>BeatO is engaged in the business of providing care for diabetic patients. Given the epidemic-level of spread of diabetes in India, this is a unique service which has shown to improve the health outcomes in 3 months by using interventions like training, coaching and regular health check-ups. While BeatO has a direct relationship with the patient and an explicit consent about using the data, some consumers who have seen success on the platform have come back and requested them to be rated as having good/bad/fair lifestyle from health perspective. Their intent is to use such a consolidated rating, not different in concept from a CIBIL rating, to reduce the cost of health insurance. Some insurance companies have also shown interest in beginning trials with such a rating.</p> <p>Blume's view is that the derivative products which are associated with identity of a person should be allowed to be created and, with consent of the owner, shared with a willing party which could be an insurance company. In the <b>current draft of DISHA act, sharing of any data with insurance or pharma companies is prohibited. This, we believe, is not in the best interest of the innovation ecosystem we represent.</b></p> <p><b>THB</b></p> <p>THB is in the business of providing re-engagement products for the diagnostic companies. This data is used with permission from the labs and only for their own gain by THB. Once this data is anonymized, it is used in conjunction with information about the lab (location, type/standard/brand of lab etc) to provide healthcare insights to pharma companies who use it in their R&amp;D to develop new products or approaches to solve healthcare problems.</p> <p>In the <b>current draft of the law, any engagement with a pharma or insurance company, even if that happens from the broad perspective of healthcare delivery in the country, is prohibited.</b> Blume's view is that <b>as long as the data is being properly anonymized, and all security related regulations are being thoroughly honoured, commercial usage for the purposes by pharma companies and public health use cases should be allowed.</b> The regulators should be impressed upon to come up with clear guidelines on what should be allowed and under what conditions. As long as clear guidelines are given, companies like THB should be expected to take a specific license (for example, a Health Information Exchange license).</p> <p><b>HealthifyMe's chatbot:</b> a network of coaches, dieticians and nutritionists who deliver customized weight loss programs to their customers. They use it by taking information about the customers' diet information, exercise details (sometimes syncing with their health devices like Fitbit), demographic information among other things. Since the chatbot is a derivative product and is being used primarily without any significance to data by any single customer, <b>Blume's view is that this should be allowed like in the cases above.</b></p>	<b>Express the view that this section restruct the scope of innovation</b>	may taken for discussion



Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
51	Cyber Blog India	Chapter 3 of Part II. DISHA, sub-section (a) & (d) of Section 3 Section 3(1)(j) Section 3(1)(m)	<p>It has been a pleasure to review the draft on Digital Information Security in the Healthcare Act (herein referred as DISHA) in the last four weeks. Undoubtedly, India is one country which is in the dire need for a data protection framework. With the Committee of Experts chaired by Justice BN Srikrishna publishing the whitepaper on Data Protection Framework for India (herein referred as the White Paper) in December 2017, the wheels have been indeed set in motion. And with the introduction of the draft bill of DISHA, India's data protection regime will definitely head in the right direction.</p> <p><b>Please find our comments in the form of below-given bullet points:</b></p> <p>Related to the <b>notion of identifiability</b>, the White Paper has discussed <b>pseudonymisation and anonymisation</b> in Chapter 3 of Part II. DISHA, on the other hand, discusses <b>anonymisation and de-identification</b> under sub-section (a) &amp; (d) of Section 3 respectively. Considering that the <b>concept of pseudonymisation and de-identification</b> are same, the definition of <b>pseudonymisation can be included in Section 3(d) in place of de-identification to bring the coherency with the proposed data protection framework.</b></p> <p>In Chapter 1 of Part III of the White Paper, failure of consent has been discussed. Although DISHA has included the <b>concept of proxy consent</b>, there is no specific provision dealing with the failure to secure consent.</p> <p>As defined in Section 3(1)(j) of DISHA, the <b>definition of an owner</b> includes an individual whose data has been generated and processed under this act. To bring this definition at par with EU-GDPR and the White Paper, the scope of definition can be expanded by using the words stored and transmitted or as may be deemed fit. <b>As per our observation, the existing proposition is not sufficient.</b></p> <p>As defined in Section 3(1)(m) of DISHA, the definition of a relative gives priority to an owner's siblings or owner's spouse's siblings before the owner's children. An additional <b>sub-clause can be added after/before Section 3(1)(m)(ii): parents of the owner so that the children of an owner get a higher priority.</b></p> <p>The scope of the <b>definition of data security</b> given under Section 3(1)(n) of DISHA <i>can be further extended by adding following words after "information in confidence" - "along with preventing unauthorized access, use, disclosure, disruption, modification, or destruction."</i></p>	Suggestion are based on comparison with <b>WHITE PAPER</b> published by the Committee of Experts chaired by Justice BN Srikrishna on <b>Data Protection Framework for India</b> (herein referred as the White Paper) in December 2017 and some with Article 13 of EU-GDPR	<p>The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.</p> <p>Competent Authority may take decision in consultation of Legal Expert</p>
		Section 30(2)	<b>Article 13 of EU-GDPR</b> prescribes the information to be provided when personal data of an individual is collected. <b>Same has been given under Section 30(2) of DISHA as it lays down the procedure for collecting the digital health data of an owner. However, Article 13 makes it mandatory to provide the information about the supervisory authority and the period for which the personal data of a data subject will be stored.</b> On the similar lines, <i>two sub-clauses under Section 30(2) can be added for providing information about the concerned State eHealth Authority (SeHA) and the period for which the digital health data of an owner will be stored.</i>	Suggesting the addition of two sub-clauses under section 30(2) for providing information about the concerned State eHealth Authority (SeHA) and the period for which the digital health data of an owner will be stored.	May be taken for discussion
		Section 37 & 38	An additional duty can be prescribed for the clinical establishments collecting the clinical health data of minors. <b>It shall be the duty of clinical establishments to verify that the consent for a minor has been lawfully provided by his guardian.</b> Section 38(e) classifies repeated data breaches by a clinical establishment or a health information exchange as a serious breach. However, <b>there is no provision under either Section 38 or Section 37 dealing with a single incident of data breach by a clinical establishment or a health information exchange. As per our suggestion, Section 37 should penalise entities and other healthcare establishments as in Section 38 for an incident of a normal breach as well.</b>	<p>Suggesting additional duty to be added for the clinical establishments collecting the clinical health data of minors</p> <p>Section 37 should penalise entities and other healthcare establishments as in Section 38 for an incident of a normal</p>	May be taken for discussion
		Section 41	Section 41 of DISHA only talks about the situation when one obtains digital health data of an owner when he is not authorized to under the provisions of DISHA. In addition, the <b>act of sharing information with a person or a party not authorized under the provisions of DISHA should also be criminalized. Although it might be a logical deduction, it would make more legal sense to explicitly mention the aforesaid.</b>	Suggesting that act of sharing information with a person or a party not authorized under the provisions of DISHA should also be criminalized.	May be taken for discussion

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
52	<a href="#">Medicea</a>	Chapter IV, Section 24, 8, d	It will help to categorically <b>define the health conditions that may be considered "Health Emergency"</b> . In the event <b>"Health Emergency" is left to interpretation, that may give rise cases which will be hard to legally prove.</b>	Need to define Health Emergency	May consult with legal and Health IT expert
		Chapter IV, Section 29, 5	A number of <b>pharmaceutical companies use the patient health data for advancement of drug research</b> and in many cases for adverse drug reporting. Given there is a blanket ban proposed on transfer of digitized health data (even if anonymized), this <b>may create hindrance in long term care and medical research.</b> We therefore <b>propose to eliminate the restriction from "ANONYMIZED" health data transfer.</b>	This act restricted the scope of research, advancement etc.	
		Schedule I	The list of data elements falling under the category of <b>"Personally Identifiable Information" is too broad</b> and therefore can have far devastating consequences for providers and healthcare establishments. Take for example the following cases – 1. Leakage of "Password" without any association of email is meaningless 2. Leakage of "Name" without any association of medical history is meaningless 3. Leakage of vehicle number without any association with medical history is meaningless. 4. A data leak of Name OR Email Address without the corresponding person's medical record can fall under the purview of the law whereas this doesn't really breach a patient's privacy Therefore we observe that the <b>Schedule I needs to be drafted well and more like US HIPPA</b> , unless the data leakage is such that a patient's medical record can be geographically and uniquely linked to the patient, it should not come under the purview of this ACT.	Suggestion on Personally Identifiable Information with reference of HIPPA Actt of US	

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
53	<a href="#">IIT Students</a>	Chapter IV point 31(3)	While <b>privacy of the patient's data is a priority, the ownership of the data must be also made very clear.</b> This shall help ensure that private clinics/hospitals/concerned entities do not misuse the data and serve as hurdles towards the dissemination of the medical data. Especially in <i>Chapter IV point 31(3), the entity is mentioned to be the custodian of the data. But can the data be shared outside of the entity if the patient from which the data was collected so wish?</i>	requested for clarity on ownership of the data	This is an Act and necessary guideline may be developed by the Authority Custodian may be defined in the Act
		Chapter II	<b>How shall the National Electronic Health Authority of India make the data available to the public/institutions/companies/labs?</b> Will it be required to obtain permission from every user for his/her health record? In my personal opinion, <i>as long as a user has given permission for usage, the health data can be made available in the public domain (either as open source or a subscription plan).</i>	Need clarity on Role of NeHA and consent of patient	Will covered under NeHA
		General	<b>The patients be allowed to choose to make all/select digital health data anonymous.</b> The Authority can emulate the Creative Common (CC) licenses used for sharing data on the Internet. This shall make data accessibility more manageable and practical.	Expressed view on Consent	No action required
		General	<b>Does the digital health data also encompass organs donated by a patient?</b> Is there a possibility of institutions other than the organisation to which the organ was donated to use the organs for research purpose? <b>Who is the owner of the donated organ or body part?</b>	requesting clarification on organ donation	already defined under Section 3 e (iii)
		General	<b>It is also not clear if a third party (researcher/company/academic institution etc.) can seek to obtain specific medical information (related to a disease, for example) from the Authority that might not be otherwise available.</b> For instance, <i>can they request for surveys from patients through the health data available?</i>	<b>Need to clarify here :</b> -Process through which digital Health data can be used for research purpose by researcher/company/academic institution etc. -If it come under NeHA purview?	This is an act detailed guidelines for roll-out would be developed by the authority.
		General	The digital health data be standardised to a fixed format making universal usage and data exchange seamless.		Standards would be defined by the Authority. This is an act detailed guidelines for roll-out would be developed by the authority.
		Chapter IV of the draft, point 29(5)	In Chapter IV of the draft, point 29(5) mentions that the digital data be not accessed or used for commercial purpose. Does this mean that a product or solution obtained from the usage of the digital data cannot be made commercially available? <i>If no, then what is the ownership and stake of the patient in the commercial product/solution?</i> <i>An accessible medical database has huge opportunity for entrepreneurs and commercial usage shall provide more impetus to medical and healthcare research.</i>	Seeking clarification on commercial usages of data	This is an act detailed guidelines for roll-out would be developed by the authority.
		General	While on one hand <b>DISHA should provide security to the patient's data, it should also not end up making the whole process closed and cumbersome for other stakeholders. The patients need to be encouraged to participate and contribute towards adding to the database. Rather than being scared in sharing their data and keeping it non-public, they can be given incentives such as a better health insurance.</b>	Expressed concern about insecurity of sharing data among general public and further suggesting to incentivise it for better health insurance	<b>may be taken for discussion</b>

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
54	CUTS International	NA	<p>CUTS Comments on draft Digital Information Security in Healthcare Act (DISHA), 2017</p> <p>At the outset it is submitted that an overarching data protection law is being drafted by the <b>Srikrishna Committee</b>, which would apply to all sectors. <i>Having a separate law for digital health data would demand a strong justification</i>. It is true that health related data are sensitive personal data and deserves extra protection and attention. However, <i>it would be wise to first wait for the overarching draft bill on data protection to come out in public domain and if the suggested regulation of the present draft Act is not reflected in the same, a decision to whether have a separate law or to amend the overarching bill can be taken at that stage.</i></p> <p>Without prejudice to the above-said, CUTS appreciates recognising that the individual whose digital health data is generated as "owner" of the data. It is a good step forward as far as establishing ownership over data is concerned. <i>However, we feel that the regulatory design is a on heavy (including national and state level authorities) side.</i> The job may need lesser members and a light regulatory design.</p> <p>In addition, if there would be an overarching authority for data protection, some role that can also play with respect to health related data.</p> <p>Therefore, it is better to wait for that law to come up, and this draft Act could be fine-tuned accordingly. Even extra need for protection of health related data could be part and parcel of the upcoming overarching law on data protection.</p>	<p>Suggesting to wait for law drafted by <b>Srikrishna Committee</b> on Data Protection</p> <p>Also Structure of Regulatory body need to re-design and suggesting additional "Overarching Authority" to constitute</p>	<p><b>The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.</b></p>

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
55	<a href="#">BLIP Initiatives</a>	Sections 3(a), 3(d), 3(k) define Anonymization, De-identification, and Personally Identified Information respectively	<b>Anonymization and deidentification</b> are interchangeably used, despite clear difference in their meanings. Anonymized data is clearly a safe form of data with no risk to anyone's privacy. The uses of <b>anonymization and de-identification should be clearly defined</b> to enable the most appropriate use towards a variety of initiatives, including <i>but not limited to, clinical research, public health, risks prediction, treatment pathways, drug discovery, market research/ intelligence.</i>	Act should also clearly carve out the uses for which anonymized data can be used and separate this from the use of de-linked data given the potential benefits associated with such use.	Competent Authority may take decision in consultation of Legal Expert
		Section 24(8d) uses the word "Health Emergency" – but clear definition remains	It may help to categorically define the health conditions that may be considered <b>"Health Emergency"</b> . Leaving <b>"Health Emergency"</b> to interpretation may lead to misuse of sensitive patient data.	Need to define "Health Emergency".	
		Sections 29.1 (use-cases of data) and 29.5 (restricting usage by likes of insurance and pharmaceutical companies) offer some clear conflicting boundaries	29.1 lays down some clear <b>use-cases of data – many of which will eventually require participation from private organizations such as pharmaceutical and insurance – given their indispensable role in the healthcare ecosystem.</b> Role of these private organizations can always be indirectly linked back to some form of commercial gains, given these are for-profit organizations. We <b>recommend that use-cases of data be defined along the lines of identifiable and/or anonymized / de-identified datasets, and not on the lines of stakeholder.</b> For a given use-case, all the relevant organizations / stakeholders should be allowed seamless participation – since that is the only collaborative way of driving value of the given use-case.	a blanket ban on use of digital health data for commercial purposes is not necessary or fair	
		Section 30 requires Clinical Establishments to generate / collect digital health data with prior consent from owner	Strict reading of this Section implies that even during a routine doctor visit, since the medical practitioner generates private health data, he/she is required to take the consent of the owner to generate the prescription – this is unproductive and will likely reduce time to treat patients. Medical practitioners also often retain copies of prescriptions to avoid any imminent threat of medical negligence claims – <b>taking a consent every time adds on a layer of effort and time, thereby reducing doctor time to actual treat patients – his / her primary role.</b>	Limit the no. of consent to reduce the patient and Doctor time	
		Section 35 requires that any entity that has generated / collected patient data is duly bound to protect the data from likely breach and/or accidents	We believe that it may not be practically feasible to impose such an obligation on the entire chain of staff engaged in patient care across organizations who may be invariably generating private health data We <b>recommend that clear processes and protocols be defined to secure, protect, and safeguard data from accidents, and all organizations / entities be evaluated on those protocols. Any possible breach due to issues outside of the defined protocols should be dealt with on a case basis</b>	clear processes and protocols be defined to secure, protect, and safeguard data from accidents, and all organizations / entities be evaluated on those protocols.	
		Draft DISHA Act is a shorter document laying the overarching policy, however with inputs missing from new-age health-tech companies, as well as similar laws in US – that are fairly detailed and specific	We reviewed the US regulations and found such high degree of detailing to ensure data security and usage is clear and transparent. We believe there is more work to be done around DISHA– and passing an act that is not detailed – will put a lot of existing functioning of organizations in "grey" areas and lead to unrequired overheads for the entire ecosystem. Also, <b>DISHA should be reviewed in context of the existing EHR Standards of India, IT Security laws, and the upcoming Data Privacy laws.</b> There must be a clear outline if one of these documents supersedes the others. Given the initiate stages of DISHA, we would request to offer our inputs and consultation in-person to the concerned authorities. We believe that the <b>concerned authorities must incorporate inputs from the new-age health-tech companies who primarily focus around innovation, and on models that may be unconventional, however significant value-adding to the entire ecosystem.</b>	<b>Comparison with US Health Regulation</b>  Must incorporate inputs from the new-age health-tech companies who primarily focus around innovation,  We may discuss the issue if it is required at this stage or not	

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
56	<a href="#">Punjab University</a> <a href="#">Legal Studies</a>	Section 5(1), 6 (2), 8 (1) & 9(2)	Due to large number of committees and their members under given section , <b>the coordination between them is difficult and hamper the success of the act</b>	Suggestion to re-design the size of committees	May be taken for discussion
		Section 14-Officers and Other Employees of the National and State Authorities-	As we have seen that there is large number of committees. Although such committees will provide safeguard against the arbitrariness but they also <b>hamper effective and efficient work of the NeHA and SeHA. There can be clash of interests which can be detrimental to the composition of the organization</b>	Clash of interest can happened between the committees	
		Section 10 Tenure- 3 years or until 65 year	But under normal circumstances, term of government is five years, this means there shall be shift in Committees and appointments after change in government. <b>To protect tenure of Members of committees, there tenure should be increased at least to five years.</b> <b>This will ensure the continuity in decision and policy making throughout the tenure of the members</b>	Suggestion to increase the tenure	
		Section 19	<b>Health Information Exchange should be established depending on the need of area</b> and on the basis of population density and not arbitrarily on the whims and fancies of the Central Government	related to HIE establishment	
		Section 21 (2)	<b>Qualification of Chief Health Information Executive are not defined:</b> As role of <b>CHIE</b> is very important and his <b>qualifications are not defined</b> in the act and left to delegated legislation. This is very important as he has to interact with the people.	Qualification of Chief Health Information Executive	may be defined by National Authority late
		Conflict in section 12 regarding the Reconstitution of the National and State Authorities	<b>Both the sections are contradictory</b> as there is confusion regarding filling up of vacancies in office of chairperson at state level. <b>According to subsection (1), power is given to central government and as per subsection (2), power is given to the state government.</b>	Highlight the contradiction under section 12 regarding vacancy at National and State level	Section 12 may be reviewed

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
57	<a href="#">India Software Product Rounda Table - ISPIRIT</a>	Section I, Clause 3 Consent Definition	<p><b>'Consent' must be based on the ORGANS Principles:</b></p> <p><b>Open Standards:</b> The framework should use open technology and legal standards available in the country.</p> <p><b>Revocable:</b> Users must have the ability to revoke consent at a later date, by requesting the data provider, the data consumer or other entities.</p> <p><b>Granular:</b> The framework should allow users to set permissions and rights for data access at a granular level.</p> <p><b>Auditable:</b> All events in the consent flow and data flow must be digitally signed and logged using the MeitY Consent Log artifact1.</p> <p><b>Two types of consent flow events must be logged - CONSENT-CREATED and CONSENT-REVOKED.</b></p> <p>For data flow events, logs must be created for <b>DATA-REQUESTED</b> (when a new data request is received by the data provider), <b>DATA-SENT</b> (when data is sent by data provider to data consumer) and <b>DATA-DENIED</b> (when data request is denied by data provider).</p> <p>Additionally, for <b>DATA-SENT</b> event, the list of data items shared by the data provider / received by the data consumer must also be logged. These non-repudiable transaction trails shall lead to higher trust and stronger accountability.</p> <p><b>Notice:</b> The user must be notified through Email, SMS, In-App Notice, and other notification mechanisms when consent is created or revoked and when data has been requested, sent or denied.</p> <p><b>Security By Design:</b> The internal and external software and systems must be designed from the ground up to be secure. There must be end-to-end security of data (PKI, DSC, tamper detection) and it must be network agnostic and data centric.</p>	<p>General Suggestion for <b>Consent definition</b></p> <p>Data Transaction between two party must be logged created txn trail for to higher trust and stronger accountability and user should informed ny email or SMS</p>	MCI Code of ethic regulation defines the "Consent" and same may be applicable for DISHA act.
		Section I, Clause 3 (1, A & D)  'Anonymization', 'De-identification'	<p>The Act should draw a distinction between anonymized data, de-identified data, and pseudonymous data:</p> <ul style="list-style-type: none"> <li>● Anonymized data is data from which absolutely nothing can be inferred about the individual.</li> <li>● De-identified data is that from which identifiers/Pis have been removed: inferences may still be possible in de-identified data.</li> <li>● Pseudonymous data is that in which identifiers have been substituted with pseudonyms: inferences are still possible on such data.</li> </ul>	Suggestion for data 'Anonymization', 'De-identification'	Measures already taken by Legal expert group. Futher discussion may be Taken to for important aspect
		Section IV, Clause 29 (5)  Purposes of collection, storage, transmission and use of the digital health data	Since individuals are in control of their healthcare data, they <b>must be given control and empowered to consent and share it for commercial purposes so that they can access value added services that benefit them.</b> This is an <b>extremely critical aspect of Data Empowerment both individually, and as a society.</b> Instead of having a blanket restriction on sharing data for commercial purposes, certain restrictions can be placed while processing data for commercial purposes like using data to effect gender or caste based discrimination.	Data Empowerment both individually, and as a society  expressed view on Commercial usage of Health data	may be taken for discussion
		Chapter V, Clause 37 and 38 Breach of digital health data, Serious breach of digital health data	"Any person" should be replaced by "any entity"	Suggested modification	Clause 37 & 38 may be reviewed
		Chapter V, Clause 38 (1 B) Serious breach of digital health data	<b>Re Identification from De-identified data or Pseudonymous data and used for malicious purposes</b> must be considered a type of breach. (However, there must be a safe mechanism for ethical reporting of the possibility of re-identification to the concerned entities.)	Express concern in cases where breach happens relating to anonymized/de-identify data by re-identification mechanism	may be taken up for discussion
		Chapter V, Clause 38 (2) Fees/penalties in cases of breach	There <b>must be a provision to score clinical establishments (monetary fine, suspension of license, etc) based on their level of compliance using Data Trust Scores.</b> Also, there <b>must be a provision for penalising clinical establishments for non-compliance.</b> For example, hospitals that share personal data without the owner's consent should get their license (to operate as a clinical establishment) suspended.	Suggestions to add some clause i.r.t. clinical establishments	Implementation issue

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		Localisation of Electronic Health Data	It is feasible and <b>recommended to localize critical health data within a span of five years from when regulations are published.</b> There are three fundamental reasons: <ul style="list-style-type: none"> <li>● <b>National Security:</b> Fiber connections from India to the world are fragile and go through open waters eminently subject to malice with minimal effort. If critical services in India are digital (e.g. health, payments, health, commerce, finance), then we put the country at risk until such critical services are fully local.</li> <li>● <b>Data Security:</b> Data that flows through pipes and hardware not subject to Indian laws and certification is under threat of unauthorized snooping, diversion or hacking - it is much easier due to physical access to hardware or networks. It is India's duty to protect the physical and legal integrity of its citizens their organisations governance data, core financial data, legal agreements, as well as deeply personal data like health. To deliver on this right, it is incontrovertible to have data and network tenancy of such data remain in India.</li> <li>● <b>Legal Sovereignty:</b> Data in international data centers even of verified Indian residents is subject to laws of the resident country including continuous inspection, search, seizure with or without consent of courts in those countries. Private and personal data may be allowed to be mirrored or jointly served from India and only from those countries which have explicitly agreed to honor Indian law, and that country can be trusted to keep its contract through adverse times. Therefore, the right framework for ensuring sovereign data access involves:  - Consent  - Security  - Data Residency</li> </ul>	Recommended to localize critical health data within a span of five years from when regulations are published Most of the points are already covered under DiSHA	<b>Implementation issue</b> Competent Authority may take decision in consultation with legal expert if desire
		Community Owned Data and Community Rights to Crowdsourced Data	We must recognise the <b>rights of community ownership</b> in crowd sourced data. <ul style="list-style-type: none"> <li>● <b>Raw data belongs to a community</b> - open unless significant part of the community, majority of at least 33% vote otherwise, weighted by contribution. Smaller storages are exempt until their databases reach community scale (to prevent undue load on small experiments)</li> <li>● <b>Enhancements belong to innovator</b>, subject to publishing of user contributions in the same structured form and schema they have processed or stored.</li> <li>● Individual users may choose to withhold their contributions publicly (or anonymise) Subject to their contributions not being incremental and being independent of others, if there are other contributions materially on top of theirs, those cannot be withheld in a commons metaphor. In a sensor driven world, raw contributions will become more and more comprehensive and eliminate data monopolies.</li> </ul>	Requested to recognise the rights of community ownership in crowd sourced data.	Implementation issue
		Electronic Consent Manager for Data Owners	In the MeitY Whitepaper on Data Protection for India2, the Consent Dashboard has been suggested as one of the technological innovations for managing consent. In February 2017, an Electronic Consent Framework (Electronic Consent Framework – Technology Specifications Version 1.13) for enabling consent for sharing of data has been released by MeitY. A similar concept may be adopted in DISHA for management of consent. Proposed Technical Approaches based on the MeitY Electronic Consent Framework5 for Electronic Consent Flows and Data Flows: <ul style="list-style-type: none"> <li>● <b>Approach A: Centralised Approach</b> : In this approach, the Consent Collector manages the consents from the users to any data request. When Data Consumer requests for data the Consent Collector validates it against the consent artefacts; collects the data from the required Data Providers and route it to the Data Consumer. The Consent Collector acts as trusted central entity and required to ensure the security of data and the privacy of the Data Owner.</li> <li>● <b>Approach B: Centralised Approach (with Central Switch)</b> : In this approach Consent Collector manages the consents provided by the user for any data requests. When a Data Consumer sends a data requests, the Consent Collector validates it against the consent artefacts and sends that requests to the Data Provider which provides the data directly to the Data Consumer. Here the consent and the data flow are separate. Data flow happens directly from Data Provider to the Data Consumer.</li> <li>● <b>Approach C: Decentralized Approach:</b> In this approach the Consent Collector manages the consents and stores the hash of the artefact in a distributed ledger. Data Consumer requests the data directly from the Data Provider which then validates the consents and serves the data. The data hash is also recorded in the ledger. The ledger helps in maintaining integrity, traceability and non-repudiability of all transactions.</li> </ul>	Consent related suggestions	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.
		B. Health Information Exchanges must be based on Open APIs	The framework for Health Information Exchanges should provide an open and standard set of application programming interfaces (APIs) for creating, accessing and updating records in EHRs, as proposed in the Policy for Open APIs by MeitY . The API definitions should be, simple and follow the principles of minimalism and privacy by design. In February 2017, the Ministry of Electronics and Information Technology (MeitY) put forward the Digital Locker Framework (Digital Locker Technology Framework – Version 1.17) as a national standard for federated storage and exchange of data. The same may be considered for the Open API definitions of Health Information Exchanges, Data Providers (Clinical Establishments), and Data Consumers (Clinical Establishments and other Entities).	Suggestion formation fo HIE	Implementation and technical issue may be consider while drafting the guidelines by NeHA



## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
		C. Health Data must be Verifiable through Digital Signatures and Standardised through a National Health Data Dictionary	All health data must be digitally signed by the source. This ensures integrity and non-repudiability of the data, creating transparency and accountability in the entire ecosystem. Also, all healthcare data must be published in an approved machine readable format with link to a deemed schema or schema bundled with data (UDL).	Expressing view on Health Data must be Verifiable through Digital Signatures and Standardised through a National	Implementation and technical issue may be consider while drafting the guidelines by NeHA
		D. Creation of a National Health Analytics Framework through Open Data and Data Sandboxes	<p>The National Health Analytics Framework must enable the creation of anonymised and aggregated datasets that assist in the creation of dashboards, reports, and other types of statistics. These aggregated datasets should present the overall direction of health of the country/state/district leading to data-driven decisions and targeted policymaking in the health sector.</p> <p>In alignment with the National Data Sharing &amp; Accessibility Policy (NDSAP)<sup>8</sup>, open datasets should be published as part of this framework to increase transparency, accountability, civil society engagement, and innovations in service delivery.</p> <p>The creation of an open data sandbox containing anonymised datasets would be a very positive step in the enablement of new data-driven businesses as well as introduction of newer services that deliver better customer value. Also, the regulators and government have a significant amount of data that can be anonymised and included in the open data sandbox that would further improve transparency and development of newer services.</p>	Suggesting Creation of a National Health Analytics Framework through Open Data and Data Sandboxes	Implementation and technical issue may be consider while drafting the guidelines by NeHA

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
58	<a href="#">The Centre for Internet and Society</a>	Stated Aims and Objectives Section 22(1)e Section 45 and 46	As stated, the <b>Digital Information Security in Healthcare Act</b> provides for establishment of National and State eHealth Authorities and Health Information Exchanges; to standardize and regulate the processes related to collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security of digital health data and such other matters related and incidental thereto. As stated, the purpose of the Digital Information Security in Healthcare Act is to facilitate the establishment of the National and State Electronic Health Authorities and Health Information Exchanges, that are in charge of standardising and regulating the process of data collection, storage and transmission. <b>This part of the Act fails to mention that the Act also prescribes the formation of a National Executive Committee and a State Executive Committee. Additionally this section fails to establish the fact that the Act also lays out the rights of the data owners, which this Act centers around.</b> Furthermore, the Act contains provisions beyond its stated purpose. These include: a) The function of the National Electronic Health Authority to "lay down the protocol for transmission of digital health data to and receiving it from other countries". (Section 22(1)(e)) b) The establishment of the Central and State Adjudicatory Authority for the purpose for adjudicating over complaints regarding the breach of digital health data (Section 45 and 46).	<b>Recommendation:</b> The stated purpose of the Act should mention the formation of the National and State Executive Committee as well as the Central and State Adjudicatory Authority. The stated purpose of the Act should inform the reader that it contains the rights of the data owner as well as address other relevant aspects of the Act.	Covered in the Act  Refer to Clause 6 (1) and 9 (1) for NeHA, SeHA Refer to Clause 28 for rights of the owner of digital health data
		Section 2	Section 2 explains the commencement and application of the Act. <b>Comments:</b> This section states that different dates may be appointed for different states and different provisions of the Act. <b>This leaves the effective commencement of the Act in ambiguity, if the Act is not uniformly applied in India the question of portability and use of digital health data will be ineffective.</b> With regard to the statement that different portions of the Act might come into force on different dates, this might cause some compromise on the security and privacy of the digital health data of the owner.	<b>Recommendations:</b> It can be understood that different states in India are in varying stages of digitization. For this reason, the Act might not be effective if applied, although implementing the Act in all the States at once would help in cases of patients moving from one state to another. <b>The provisions of the Act need to be effective uniformly to reduce confusion as well as to ensure that the data, privacy and security of the people are not</b>	Implementation issue. May be taken up for discussion
		Section 3 Section 2(1)(h) Section 28 Section 19 Section 20 & 21 Section 3(1)(i) Section 3(1)(d)	Section 3 defines the terms used in the Act The term 'direct care' needs to be defined. The term is first used in the proviso to Section 29, which states "Provided that personally identifiable information may only be used for the purposes of direct care of the owner of the data, as specified in clauses (a) to (c) of sub-section (1), subject to provisions of section 28, to the extent considered necessary, and in the best interest of the owner." It is crucial that the Act defines direct care especially when it is with respect to the use of personally identifiable information. The term 'Health Information Exchange' as defined under Section 2(1)(h) is vague and it does not clearly explain the body formed under this Act. Section 19 of the Act states that the central government shall establish health information exchanges; and the following section 20 and 21 deal with the management of the exchanges and the powers and functions of the Chief Information Executive. <b>The Act fails to state what the Health Information Exchange is, and as various provisions of the Act group clinical establishments and health information exchanges together, there needs to be a more detailed definition of it.</b> In the definition of 'Clinical Establishments' under Section 3(1)(i) it is stated as follows "but does that include clinical establishments owned, controlled or managed by the Armed Forces". <b>There seems to be a typographical error and the part should read as "but does not include clinical establishments owned, controlled or managed by the Armed Forces".</b> As the use of the word 'but' suggests an exception, it needs to be made clarified so as to remove ambiguity. The term "De-identification" that is defined in Section 3(1)(d) is <b>not used anywhere outside the definitions clause and should be removed</b>	Some of the terms are incomplete and a few of the terms used in the Act have not been included in the list of definitions.  typographical error	Clause 3 (i) (e) may be reviewed.  Scope/purpose of Health Information Exchange (HIE) may be provisioned.  May be taken up for discussion.
		Section 5	Section 5 This provision addresses the composition of the National Electronic Health Authority Of India. <b>Comment:</b> The National Electronic Health Authority is the apex body that is responsible for not only setting standards and protocols for the generation, collection, storage and transmission of the digital health data, but also to ensure that steps are taken to maintain the privacy and security of the data. However in the composition of the Authority there is no member who specialises in security, or a Chief Security Officer. <b>Recommendations:</b> One of the primary objectives of the Authority is to safeguard the privacy and security of the data. For this reason there needs to be an officer appointed specifically to advise and decide on strategies to improve privacy and security. For example Section 3001 of the (American) Health Information Technology for Economic and Clinical Health Act" (HITECH Act) of provides for the appointment of a Chief Privacy Officer whose duty is to advise the National Coordinator on privacy, security, and data stewardship of electronic health information.	needs to be an officer appointed specifically to advise and decide on strategies to improve privacy and security	Implementation issue. May be taken up for discussion

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Section 6	Section 6 addresses the composition of the National Executive Committee <b>Comments:</b> With regard to the composition of the of the committee members, Section 6(1)(d) states that the Committee shall be 'supported by consultants and ehealth section.' <i>This sentence is vague as well as the number of consultants that are to be appointed is not mentioned.</i> <b>Recommendations:</b> This section should clarify what 'e-health section' is and define it in case this entity has been formed for the purposes of this Act. The number of consultants also needs to be stated. If not a precise number, the section should state the upper limit to the number of consultants that can be appointed.	This section should clarify what 'e-health section' is and define it in case this entity has been formed for the purposes of this Act.	may be taken up for discussion
		Section 8	Section 8 lays down the composition of the State Electronic Health Authorities <b>Comments:</b> Regarding the composition of the State Electronic Health Authorities, Section 8(1)(d) specifies the appointment of three ex-officio members. This clause states that the three ex-officio members to be appointed by the State Government should be from the 'Director, State Health Services; from the State Information Technology department; and from the State Law department. <b>The composition of this authority is different from the National Authority.</b> The National Authority comprised of four ex officio members the addition being a representative from the Ministry of Panchayati Raj or Ministry of Women & Child Development. <b>This representative is missing from the State Electronic Health Authority.</b>	Recommendations: There needs to be representation ideally from both the local government bodies and also from members who have worked on issues relating to women and children. This representation is required to ensure a more diverse set of expertise in looking at various issues that might arise with respect to digital health records	may be taken up for discussion
		Section 9	Section 9 addresses details of the formation and composition of the State Executive Committee <b>Comments:</b> In the composition of the of the Committee members, Section 9(1)(d) states that the Committee shall be 'supported by consultants and ehealth section.' <i>This term is vague as well as the number of consultants that are to be appointed is not mentioned.</i>	Need to clarify what 'e-health section' means as well as define a number of such consultants that are to be appointed by the Committee.	may be taken up for discussion
		Section 16	Section 16 explains the disqualifications of the members of the National Electronic Health Authority or a State Electronic Health Authority. <b>Comments:</b> In Section 16(1)(ii) the clause stipulating the disqualification of the members reads as follows "Is an undercharged insolvent". <i>This seems to look like an typographical error.</i> <b>Recommendations:</b> The clause should read as "is an undischarged insolvent, as can be seen from other legislations that have provisions that detail disqualifications criterias. For example in the Consumer Protection Act in the composition of the District Forum (Section 10(1)(iii)(a) states that the member of the District Forum shall be disqualified as a member if he is an "is an undischarged insolvent". Section 16(1)(ii) of the Act should be edited accordingly, though if the clause is meant to read as stated the Act should provide a definition of the term.	typographical error.	Clause 16 (ii) may be reviewed and taken up for discussion.
		Section 21	Section 21 explains the appointment of The Chief Health Information Executive and his functions. <b>Comments:</b> Section 21(2)(b) states that the Chief Health Information Executive (CHIE) is the data controlling authority of the health information exchange and is responsible for the smooth functioning of the exchange. In order to ensure this, <b>the CHIE has the power to access and process the digital health data that is transmitted by the clinical establishments, for the transmission of the digital health care data.</b> <i>Although the Act states that theses powers will be according to the norms prescribed by the National Electronic Health Authority of India, until these norms are introduced the CHIE will be accessing the data .</i>	the functioning of the CHIE, his powers and functions must be formulated at the earliest	
		Section 22	Section 22 explains the delegation of powers and functions to the National Electronic Health Authority of India. <b>Comments:</b> This section delegates a number of functions to the Authority that places it in the role of a manager and regulator for issues pertaining to digital health data including periodically overseeing the functioning of the health information exchanges etc. <b>Recommendations:</b> The functions of the Board should be limited to developing standards and protocols, safeguarding privacy and other rights, ensuring public transparency, promoting information and debate and a few other limited functions necessary for a regulatory authority. Towards this, the Board should be comprised of separate Committees to address these different functions. At the minimum, there should be a Committee to oversee the workings of the health information exchanges as well as one to handel breaches in security.	the Board should be comprised of <b>separate Committees to address these different functions.</b> At the minimum, there should be a Committee to oversee the workings of the health information exchanges as well as one to handel breaches in security	
		Section 28	Section 28 lays down the rights of the owner of the digital health data. Section 28 (1)(e) states that the data owner has the right to prevent any transmission or disclosure of any 'sensitive health related data'. The <b>term sensitive health related data has not been defined under the Act</b> , however the <i>Act defines sensitive health related information under Section 3(1)(o).</i>	Recommendation: This clause should read as "The right to prevent any transmission or disclosure of any 'sensitive health related information' that is likely to cause damage or distress to the owner.	

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Section 28(7)	<p>Section 28 (7) of the Act states that the “owner of the digital health data shall have a right to access their digital health data with details of consent given and data accessed by any clinical establishment/entity.</p> <p><b>Comments:</b> The Act fails to explain how the data can be accessed by the data owner, through an online portal, an app, data centers etc. The act also lacks a provision that ensures that a copy of the digital health data is provided to every data owner.</p> <p><b>Recommendations:</b> The Act should <b>specifically state how the data can be accessed by the data owner. Additionally, the owner of the data must be provided with a copy of his healthcare data. Either in a printed format or available online for download.</b> This is a necessary right of the owner of the data. This helps in making informed decisions regarding the use of data as well holds the data custodian accountable. <i>This also helps in tracking errors in a person's records. This data should also be available within a prescribed time</i></p>	Act should specifically state how the data can be accessed by the data owner	
		Section 37	<p><b>Section 37 discusses the breach of digital health data</b></p> <p><b>Comments:</b> This section while stating what qualifies as a breach of digital health data as well as the punishment for the same <i>fails to mention the measures that are to be taken once the breach is detected as well as the measures to mitigate the breach.</i> Section 21(2)(d) states that the Chief Health Information Executive has to notify the data breach to the owner and ‘such other concerned’ and <b>Section 35(5) also states</b> that the clinical establishment or a health information exchange shall inform the owner of the data of the breach immediately and not later than three working days. <i>However the Act does not explicitly state that the breach has to be notified to the apex bodies i.e the Sta and Neha.</i></p> <p><b>Recommendations:</b> This <b>section should also specify that the breach will be notified to the apex bodies immediately as well as lay down step for control and mitigation of the breach.</b></p> <p>For example, HIPAA breach notification rule 45 CFR 164.400 et seq which states that “If Public Health Information(PHI) is disclosed in violation of its policies and procedures, a covered entity must mitigate, to the furthest extent actionable, any harmful effects.” Additionally HIPAA also requires that in case of a breach the health care provider has to notify the Secretary of Health and Human Services. It also states that if a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. As breaches such as cyber attacks do not happen in isolation and can affect a number of centres at once, this requirement helps individuals know that there has been a breach as well as help keep the data custodians accountable.</p>	This section should also specify that the breach will be notified to the apex bodies immediately as well as lay down step for control and mitigation of the breach.	
		Sections 45 and 46	<p><b>Sections 45 and 46 These provisions deal with the complaints to the State Adjudicating Authority and the Central Adjudicating Authority respectively.</b></p> <p><b>Comment:</b> While these two sections provide for recourse that the data owner can take in case of any breach of his data. Some of the provisions are limited, for example the complaints can only be made on account of a breach of digital health data. This fails to consider complaints that might not come under the definition of breach under the Act. These can be for example, the refusal to provide digital healthcare information, the failure to remove records after withdrawal of consent etc. <i>Although Section 37(1)(b) includes anything done in contravention of the exclusive right conferred upon the owner of the digital health data as a breach .</i></p> <p><b>Recommendations:</b> This section should lay down in detail the issues which the data owner can seek redressal from and not limit its scope only to breaches.</p>		

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		<b>General</b>  <b>Section 35(1))</b> <b>section 43A</b>	<p>The digitization of health records, adoption of national standards for electronic health records and use of healthcare data for research represents a significant public interest opportunity for Digital India. We note with appreciation the privacy and security reasons in the Draft Digital Information Security in Healthcare Act.</p> <p><b>Privacy Safeguards :-</b> However, <b>the proposed Act does not contain provisions for instances where the digital health data of the owner has been collected without his/her consent, neither does it mention the status of the data when the owner withdraws their consent.</b> The Act states that the data can be withdrawn by the owner but <i>it does not state the manner in which the data will be deleted from the records and/or if any copy would be maintained as a record by the custodian of the data.</i> There are also <b>issues with respect to the right to privacy and its violation thereof due to the non-consensual collection of health data. This is an issue which needs to be addressed in this Act.</b> It should not be left unaddressed as this would only result in a lack of clarity which would require protracted court cases to resolve.</p> <p>Presently, the proposed Act is being introduced without comprehensive privacy safeguards in place on issues such as consent, collection, and retention of data. Though the National Electronic Health Authority is responsible for safeguarding the privacy, security, and confidentiality of the digital health data of the owner (Section 35(1)) - it is not adequate given the fact that India does not have a comprehensive privacy legislation. Though section 43A and associated Rules of the Information Technology Act would apply to the collection, use, and sharing of digital health data by the National and State Electronic Health Authority as well as clinical establishments and other entities (as they would fall under the definition of 'body corporate' under the IT Act), the Health Information Exchange would not clearly be body corporate as per the IT Act and would not fall under the ambit of the Acts provisions or Rules. Safeguards are needed to protect against the invasion of informational privacy and physical privacy at the level of these controlled bodies which are controlled by the National Electronic Health Authority.</p>	<p>1) the proposed Act does not contain provisions for instances where the digital health data of the owner has been collected without his/her consent, neither does it mention the status of the data when the owner withdraws their consent.</p> <p>2) issues with respect to the right to privacy and its violation thereof due to the non-consensual collection of health data. This is an issue which needs to be addressed in this Act</p> <p>3) proposed Act is being introduced without comprehensive privacy safeguards in place on issues such as consent, collection, and retention of data</p> <p>4) <b>Health Information Exchange would not clearly be body corporate as per the IT Act</b> and would not fall under the ambit of the Acts provisions or Rules. Safeguards are needed to protect against the invasion of informational privacy and physical privacy at the level of these controlled bodies which are controlled by the National Electronic Health Authority</p>	
		<b>General</b>	<p><b>Annual Public Reporting :</b> The Act does not require the National or even the State Electronic Health Authority to disclose publicly available information on an annual basis regarding the functioning and financial aspects of matters contained within the Act. Such disclosure is crucial to ensure that the public is able to make informed decisions. Categories that could be included in such reports include: Number of digital health records added, total number of records contained in the database, number of records deleted from the database, the number of health information exchanges established, the number of records that are transmitted internationally, and the number of data breaches, to name a few.</p>	<p>The Act does not require the National or even the State Electronic Health Authority to disclose publicly available information on an annual basis regarding the functioning and financial aspects of matters contained within the Act</p>	

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding/Remarks	Remark
59	Su-swa Consultants	General	<p>At the outset, it is noted with immense appreciation that MoHPW has placed in the public domain, for comments and suggestions, its plans to set up a nodal body in form of "National Digital Health Authority" as a statutory body for promotion/ adoption of e-Health standards; to enforce privacy &amp; security measures for electronic health data; and, to regulate storage &amp; exchange of Electronic Health Records. The purpose as mentioned in the preamble to the Act is laudatory in that it seeks to provide for electronic health data privacy, confidentiality, security, and standardization.</p> <p><b>comments</b></p> <p>It is worth noting that <b>India does not currently have an overarching Act to deal with Data Protection</b>. While the Government has made substantial efforts in moving in this direction in accordance with international laws and best practices, and in pursuance of several rulings and a landmark judgement by Hon. <b>Supreme Court of India recently, a general-purpose Data Protection law based on cardinal principles of data privacy, confidentiality and security has eluded us so far.</b></p> <p>Presently, there exists a plethora of Acts, rules, regulations and executive orders that deal with privacy principles, practices, and related offences in various domains – the most recent addition to this being the enactment of the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016. It appears necessary, in the first instance, <b>to homogenize different policy documents to ensure that there is consistency amongst the provisions of these legislations, as well as a general compliance with the defined principles of data protection.</b></p> <p>A sectoral (or fragmented) approach that deals separately with each particular vertical, however important that vertical may be, cannot be an ideal approach to ensure the larger purpose of data protection. <b>To that extent, the present initiative of DISHA is premature. A Data Protection Act should first be enacted that is based on defined principles of data protection, and allow specific sectors (such as DISHA in the health sector) to develop, or use already developed privacy standards.</b> Once an overarching Act becomes law – other laws with privacy implications may ensure that sectoral variations are retained within the framework of broad harmonization and compliance with defined principles.</p>	in general suggested, First National Data Protection Law should be enacted then go for this kind act.	
		Section 31 (1) Section 31 (2)	<p>Comments specific to DISHA</p> <p>As stated in the preamble to the draft DISHA Bill, this legislation is more focused on regulation than on the development of digital information the Healthcare sector. It is common knowledge that the extent of digital information in the healthcare sector is rather limited. In this nascent stage of digitization of healthcare data, there needs to be a substantive encouragement, and incentives, to ensure that the extent of digit health data grows exponentially. <b>The present thrust at regulation before development may actually become counter-productive, in that it may discourage the process of digitization itself!!</b></p> <p>It is heartening to note that in the draft DISHA, the ownership of digital health data (DHD) has been vested in the individual. Section 31 (1) provides that <b>"the digital health data generated, collected, stored or transmitted shall be owned by the individual whose health data has been digitized"</b> but what is given by one hand is withdrawn by the other! <b>The individual is the "owner" but not the "controller" of her own DHD.</b> Section 31 (2) provides that "a clinical establishment or Health Information Exchange shall hold such digital health care data referred to in sub-section (1) above in trust for the owner" and if she needs to access it, she must obtain the permission or approval of the National Electronic Health Authority of India <b>because section 34 (5) provides that "the owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India".</b></p> <p>In the interest of empowerment of the individual, it would appear <b>appropriate that she should not only be acknowledged as the 'owner' of her DHD but must also be empowered to 'control' her DHD by 'holding' and 'accessing' it in any manner she deems appropriate, and that there should not be any mandatory requirement of keeping the data 'in trust' with another entity or to seek permissions/ approval of any Authority to access one's own DHD.</b></p>	Individual should be empowered with controlling right of DHD along with Ownership; there should not be any mandatory requirement of keeping the data 'in trust' with another entity or to seek permissions/ approval of any Authority to access one's own DHD	
		Section 29 (1)	<p>Section 29 (1) of the draft Bill provides for collection, storage, transmission and use of the digital health data by clinical establishments and/ or the health information exchange, for listed purposes such as: to advance the delivery of patient centric medical care; to provide appropriate information to help guide medical decisions at the time and place of treatment; to improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data; to improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks; to facilitate health and clinical research and health care quality; to promote early detection, prevention, and management of chronic diseases; to carry out public health research, review and analysis, and policy formulation; and, to undertake academic research and other related purposes etc. <b>However, section 29 (5) of the Bill provides that the "Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose..."</b></p> <p>The term "commercial purpose" has not been defined in the draft Bill but if a general meaning of the term were to be assumed, it would be difficult to reconcile that the purposes (please see highlighted text above) for which collection, storage, transmission and use of DHD is permitted under 29(1) shall not be undertaken with commercial intent after DISHA becomes law!!</p> <p>In addition to above broad comments, we have a number of other specific suggestions for amendment to various provisions of the draft Bill, which can be submitted should the Government wish to proceed with legislation forthwith, without first enacting a National Data Protection law. We shall look forward to any opportunity that may exist to participate in the discussions towards finalization of the draft Bill.</p>	Need clarity on Term commercial use as not defined in act	

## 909695/2018/E-GOVERNANCE

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
60	Kratikal Tech	Section 28:	<p><b>Section 28:</b>  <b>Right to Retrieve:</b> The data owner should have the right to retrieve all his digital health information from the clinical establishment for taking backups, conducting independent studies etc  <b>Right to forget:</b> The data owner should have the right to demand removal of all his data from all records of clinical establishments, except in the case where it may be mandatory by law.</p>	Right to retrieve and right to forget	
		Section 32:	<p><b>Section 32:</b>            Data collected by the clinical establishment, stored digitally in software and applications which are should be quarterly audited by the means of Vulnerability assessments and penetration tests (VA-PT) to ensure security from cyber threats            Data collected by the clinical establishment should be stored within a network/cloud which is regularly audited by the means of Vulnerability assessments and penetration tests (VA-PT) to ensure security from cyber threats            Entire infrastructure responsible for storage, transmission and retrieval of digital health data including the applications used for the same will be annually audited against standard compliance like ISO 27001, Data Privacy Laws and other relevant Healthcare security best practices            Data collected by clinical establishments should be immediately anonymised using industry accepted anonymity algorithms like K-Anonymity, L-Diversity, T-Closeness, epsilon differential privacy. Also, relevant multiplicative noise to be added to ensure maximum security in case of a data breach.</p>	Audit of Data to ensure security from cyber threats	
		Section 35	<p><b>Section 35</b>            Data collected by the clinical establishment should be kept secure by ensuring security of People-Process-Technology. People are the weakest link in the security chain of any organisation, hence the clinical establishments should ensure that the employees are able to identify different types of cyber attacks by simulating variety of cyber attacks like Phishing, Cyber Scams, Smishing, Ransomware attacks etc on the employees.            As stated by RBI in their circular to all the NBFCs under INFORMATION AND CYBER SECURITY policy <b>Section 3.12</b>, human link is the weakest link in the information security chain. <b>Hence clinical establishments should be forced to conduct regular cyber security simulations on their employees to make sure that the employees are protected, thereby protecting the data of the patients.</b>  <b>Cyber Security Awareness training</b> should also be mandatory for the employees of the clinical establishments.            The clinical establishments should also make sure that their internal infrastructure, servers, medical devices, endpoints etc are secure by conducting regular Vulnerability Assessment and Penetration Testing (VA-PT).            If incorporated, these changes can go a long way in ensuring security of eHealth data. If you need any clarifications, I am always at your disposal.</p>	Data security	

## 909695/2018/E-GOVERNANCE

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remarks
61	Cyber Peace Foundation	General	<p>This is Vineet Kumar from Cyber Peace Foundation.</p> <p>About Cyber Peace Foundation</p> <p>Cyber Peace Foundation(CPF) is an award-winning apolitical civil society organisation and think tank of cybersecurity and policy experts. CPF is involved in Policy Advocacy, Research and Training related to all aspects of Cyber Peace and Cyber Security. Key areas of it's work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organizations, academic institutions and civil society entities.</p> <p>Cyber Peace Foundation was formed with the vision of pioneering cyber peace initiatives to build collective resiliency against cybercrimes and global threats of cyber warfare.</p> <p><b>Feedback from our Policy Team on the DISHA Act (Draft)</b></p> <p>On perusal of the proposed Digital Information Security Act (DISHA), it has been noted that there is a <b>need to clearly define the parameters of access being given to law enforcement agencies in case they need to access the data collected</b>. One possible instance where the law enforcement agency would need such access is in case of verifying medical conditions of convicts in case they need treatment during the course of their incarceration. There is a <b>need to ensure that the data collected by the law enforcement agencies cannot be used for any purpose other than the one specified in the proposed Act</b>.</p> <p>Provisions may further be <b>drafted to aid law enforcement agencies in criminal investigations with the use of the data collected, subject to conditions of non-disclosure to third parties</b>. However, it is pertinent <b>to ensure that health data is not shared with the law enforcement agencies except by the way of a Court order to this effect. The proposed Act, in its current form, lacks any provision to this effect.</b></p> <p>We came across the draft yesterday and couldn't do a detailed study. We would request you to extend the deadline by 14 days so</p>		



Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
62	<a href="#">Bill &amp; Melinda Gates Foundation</a>	General	<p>1. It is not clear how does this Act will relate/align to the upcoming Data Protection law and how any conflicts with the Data Protection law shall be sorted out. This will require clarity and possible amendments when the Data Protection law is approved.</p> <p>2. It is recommended for it to be mandated under the DISHA Act that a Privacy policy is created by all the entities in scope of the Act and made available to the owner(s) of Digital Health data.</p> <p>3. It is recommended to have a requirement of conducting risk assessments by various entities under the scope of DISHA Act.</p> <p>4. It is recommended for it to be mandated under the DISHA that a training and awareness program for the staff managing the Digital Health data is conducted periodically.</p> <p>5. Role of sub-contracting agencies shall be defined under the Act. Standard contractual clauses may be defined under the Act for any sub-contracting agency. Such clauses shall help in binding the agencies with the requirements of the Act.</p> <p>6. To enable an ecosystem of qualified auditors on Healthcare security and privacy, the Act may include provisions on empanelment of qualified auditors to conduct audits of the agencies in the Healthcare ecosystem.</p> <p>7. Reference to adoption of Electronic Health Record (EHR) standards may be made to ensure these are maintained by the various healthcare agencies in purview of DISHA.</p> <p>8. Responsibilities of NeHA/NDHA and SeHA may also include development and imparting of Training and awareness amongst entities in purview of DISHA.</p> <p>9. Responsibilities of NeHA/NDHA and SeHA may also include creating channels for entities and agencies to avail technical and legal guidance on implementation of the Act. The channels may include website, email, helpdesk, etc. may be created for all such needs.</p> <p>10. It is recommended for it to be mandated under the Act that a Privacy officer shall be appointed by all entities under the scope of the Act, including NeHA/NDHA, SeHA, Health Information Exchanges, Clinical Establishments, etc.</p> <p>11. Provision for reporting of data breaches by anyone may be created to provide a channel for reporting to any individual. This could be an email / link on a website / etc.</p>	Expressing concern on alignment of DISHA with upcoming Data Protection act as developed by MeitY and also give recommendation for requirement of conducting risk assessments/ training and awareness program and others	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the healthcare data protection.  -Standards would be defined by the Authority. This is an act detailed guidelines for roll-out would be developed by the authority
		Chapter No.: I Section 3 (1) (a) (d)	: Difference between Anonymization and De-identification is not clear. European Union and many other countries also have an additional concept called as "Pseudonymization". That Act shall ensure that a clearer definition for the 3 concepts is available and their relevance under the Act is clearly mentioned. Additionally, for de-identification, HIPAA (Health Insurance Portability and Accountability Act of US) mentions 2 ways to de-identify - (1) remove all of at least 17 data elements listed in the privacy rule, such as name, phone number and address; or (2) have an expert certify that the risk of re-identifying the individuals is very small. Same may be considered for providing further guidance on de-identification of data to avoid any ambiguity.	Need clarity on Anonymization and De-identification  Also highlight additional concept with reference to other country act like HIPPA and EU	
		Section 3 (1) (c)	The definition of consent may be enhanced. The new GDPR law in Europe mentions consent to be "unambiguous, freely given, specific, informed and explicit". The definition of consent requires a statement or clear affirmative action to signify agreement to the proceedings. The definition of consent may be revised to ensure that it is implemented in the right spirit and in an adequately informed manner.	Express view related to Consent	MCI Code of ethic regulation defines the "Consent" and same may be applicable for DISHA act.
		Section 3 (1) (e)	The definition of "Digital Health Data" may be linked to the IT Rules 2011 (reasonable security practices and procedures and sensitive personal data or information) where it is defined as "Sensitive personal data or information". This should be revised once the Data Protection law has been enacted.	Suggested to linkage of DHD and IT rules 2011	may be consider after due consultation with expert committee
		Section 3 (1) (f)	Examples of entities may be given to clarify whether entities such as Insurance companies or companies (collecting employee medical data) fall in scope of DISHA. In our view all entities that have access to / are custodians of any medical data of any individual, should be falling within the ambit of this Act.	Expressed view on Scope of DISHA	Already covered. No action required
		Section 3 (1) (h)	Health Information Exchange – The definition and the type of organizations that shall be Health information exchange is not clear. Same shall be clarified through examples and the governance mechanism be clarified	Need clarity on HIE	may be taken for discussion
		Section 3 (1) (k)	For now, definition of "Personally Identifiable Information" may be linked to the definition of "Personal information" under the IT Act where it is defined as "any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person". This should be revised after the Data Protection law has been enacted.	Suggested to linkage of PII to Personal information under the IT act	may be consider after due consultation with expert committee
		Section 3 (1) (o)	Any health-related data has the capability of causing substantial harm to an individual. Across the world all health-related data is generally considered sensitive personal information. There may not be a need to define sensitive health-related information separately.	expressing concern about sensitive health-related information	may be taken for discussion
		Chapter No.: II Section 5 (3) (8)	: It is not very clear how the State Electronic Health Authority relate to the National Electronic Health Authority. The governance mechanism within and between these entities should be explicitly defined and shared.	Need clarity on linkage between NEHA & SEHA	may be taken for discussion
		Section 6 (2)	: The roles and responsibilities of all the members may be defined more clearly to ensure demarcation of the jobs and activities	roles and responsibilities of all the members	NeHA will take care of it
		Chapter No.: II Section 19, 20	: Definition of Health Information Exchanges and the role of Health Information Exchanges is not clear as to which organizations will be Health Information Exchanges.	Need clarity on role of HIE	may be taken for discussion
		Chapter No.: II Section 21	: Dedicated role of a Privacy officer also may be considered.		NeHA will take care of it
		Chapter No.: III Section 22 (1) (c)	: Instead of using the word 'investigation' it can be replaced with the word 'audit/assessment/ review'. This would ensure a wider coverage in terms of ensuring compliance.	Suggest modification for word investigation	may be taken for discussion

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Section 24 (1) (b)	: Instead of using the word 'investigation' it can be replaced with the word 'audit/assessment/review'. This would ensure a wider coverage in terms of ensuring compliance.	Suggest modification for word investigation	may be taken for discussion
		Chapter No.: IV Section 28 (3)	: In case an owner withdraws her/his consent, <b>what is the provision that should be followed by the Health Information Exchange and/or the clinical establishment to ensure such data is deleted and removed.</b> Appropriate provisions need to be prepared for its archival/ deletion in a specified period of time.	Concern about Consent	may be taken for discussion
		Section 28 (8)	: <b>Timeline for rectification of data</b> after request from the owner may be defined.	request to define Timeline for rectification of data	implementation issue. National authority may consider it while drafting guidelines
		Section 28 (8) (d)	: Need to define the definition of 'health emergency' to ensure the said clause is not misused by vested interests in the absence of appropriate consent from the owner.	Need to define the definition of 'health emergency'	may be taken for discussion.
		Chapter No.: IV Section 29 (1)	: The purposes do not mention the purposes related to processing of Insurance policies or processing of employee data etc. hence creating confusion on whether entities such as Insurance companies, companies processing employee medical data fall in scope of DISHA.	Expressed view on Scope of DISHA	Already covered. No action required
		Chapter No.: IV Section 29 (5)	: <b>It is not clear whether Health data collected directly from the individuals by Insurance companies or other organizations fall under the scope of DISHA. This data mostly may be kept by the companies in digital format.</b>		
		Chapter No.: IV Section 30	: It shall be <b>clearly mentioned that consent needs to be taken prior to collection of any digital health data.</b> The Act currently mentions that consent shall be taken but it must be mentioned clearly that consent needs to be taken prior to collection of digital health data and each time it is shared/sought.	Concern about Consent	may be taken for discussion
		Chapter No.: IV Section 32	: <b>Retention period for the digital health data by NeHA/NDHA, SeHA, Health Information exchanges, clinical establishments, other entities etc. has not been defined.</b> Same should be defined under the Act along with the mode(s) of retention.	Need to defined Retention period for the digital health data	
		Chapter No.: IV Section 32, 33, 34	The Act must define the requirement of log storage for any activity performed on the digital health data. It could be generation, processing, access, transmission, deletion, consent, etc.	Need to define log storage	
		Chapter No.: IV Section 34 (4)	Competent court may be defined further; it could be a Chief Metropolitan Magistrate or Chief Judicial Magistrate, as may be appropriate.	Need to define the competent court	
		Chapter No.: IV Section 34 (6) & (7)	<b>Emergency situations shall be clearly defined to avoid ambiguity</b> and who will be the authority to decide whether a case is emergency or not. These should be pre-defined to the extent possible within the Act itself and mechanism for any new situation should also be articulated as a part of the Act.	Need to define Health emergency	
		Chapter No.: IV Section 35 (4)	The Act should also define for <b>having the security protocols defined in the rules, standards, and protocols.</b> This is important to ensure every new security provision is immediately communicated to all the stakeholders and followed by them.	Need to define security protocol	Implementation issue i.r.o of security protocol. May be taken care by NeHA
		Chapter No.: IV Section 35 (5)	<b>3 working days may be a less time for notification to owner of data especially in cases where breach involves multiple individuals. Breach notification shall be made mandatory to NeHA/NDHA, SeHA and Media based on the nature of breach. Learnings can be taken from HITECH Act of USA,</b> which has the following provisions: "In the event of breach of unsecured information, the entity in scope must conduct a risk assessment to determine the risk of harm. If there is a significant risk of harm (financial, reputational or other) from a breach, a covered entity must notify individuals within 60 days of discovery. If a "business associate" discovers a breach it must notify the covered entity. If the breach affects more than 500 people the covered entity must notify HHS immediately, and if the breach affects 500 or more in the same jurisdiction, it must notify the media."	Express concern about Data breach and share the learning of other country act like HITECH and suggesting same measure can be adopted	may be taken for discussion
		Chapter No.: V Section 37 (1) (a)	The significance of "contravention to provisions of chapter II of this Act" is not clear as Chapter II is primarily on the responsibilities of the various agencies involved in processing of Digital Health data. It is not clear whether an insurance company / TPA collecting medical information for processing a claim, is a breach or not; this should be clearly defined within the section so that there is no ambiguity left.	need clarity on significance of "contravention to provisions"	may be taken for discussion
		Chapter No.: V Section 37 (2)	: <b>A detailed guide should be provided on how the compensation is to be given to the owner/ aggrieved party in case of a breach.</b>	<b>Express the view on compensation</b>	National authority may draft the guidelines for compensation for damage/loss and also put the provision for forming investigating committee
		Chapter No.: V Section 38 (1) (d)	: <b>This requirement indicates that if insurance companies / TPA(s) process digital health data that shall be considered as a breach.</b> There is a little bit of ambiguity within the scope of DISHA in this regard.	Raise concern on processing of DHD by insurance companies	already define in act

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Chapter No.: V Section 38	<i>: The fine of INR Five lakhs as compensation may need to be relooked at .</i> Breach of digital health data causes a significant damage to individual. Even though it cannot be corrected through compensation, the amount needs to be significant enough to act as a deterrent. <i>Under HIPAA and HITECH the maximum compensation could go as high as US\$ 1.5 million for most wilful violations</i> . Additionally, an adjudicating body shall be given the powers to assess the penalties for individual complaints instead of being imposed by a court.	<b>Express the view on compensation</b>	National authority may draft the guidelines for compensation for damage/loss and also put the provision for forming investigating committee May be taken for discussion
		Chapter No.: VI Section 47	<i>: Power of Adjudicating Authority should also include powers to assess and award damages to individuals who have been impacted by data breach. Process and Rules shall be created to assess the level of damage and to accordingly award penalties.</i> This is the case with HIPAA as well where Office of Civil Rights (OCR) processes individual complaints and can assess civil monetary penalties up to US\$ 1.5 million per year per type of violation.	Suggesting Power of Adjudicating Authority should also include powers to assess and award damages to individuals who have been impacted by data breach	may be taken into discussion
		Chapter No.: VI Section 47 (3)	The member of the Adjudicating Authority should also be having a decent background in the domain of privacy.	Qualification of member	may be consider after due consultation with expert
		Chapter No.: VI Section 48 (1)	<i>: The roles of officers and employees should be clearly defined to ensure Adjudicating authorities</i> have personnel which can discharge the duties as envisaged under this Act	role of officer should be defined	may be consider after due consultation with expert
		Chapter No.: VII Section 52	<i>: How will DISHA relate to the upcoming Data Protection law needs clarity given the likelihood of the Data Protection law being an umbrella law for all kinds of data/information.</i>	express concern on DiSHA's alignment with upcoming Data Protection law	The Data Protection act as developed by MeitY provides overall framework, this act specifically targets the

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
63	<a href="#">International Institute of Health Management Research IIHMR</a>	General	1. Nomenclature: NDHA vs NeHA As per the MoHFW covering letter dt 21 Mar 2018 regarding comments on the draft Act, National Digital Health Authority (NDHA) is proposed to be set up, however, as per Section 4, Chapter II of the proposed Act National Electronic Health Authority (NeHA) shall be established.	Recommendation: Any one nomenclature be taken. NeHA is broader term thus recommended.	Now NDHA is revised as DISHA
		Para 3(1)(c): Consent	As per IT Act 2000, any electronic document which is not digitally signed is equivalent to unsigned paper document. However, Consent (in physical or paper form) has to be signed by an individual, thus Consent taken in electronic form should be digitally signed.	Recommendation: Paragraph may be amended as below 'Consent' means expressed informed consent, whether in written or electronic form (duly digitally signed), given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data.	may taken for discussion
		Para 3(1)(c): Digital Health Data	Following may be added: (a) EMR/EHR. (b) Lab reports. (c) Radiographic reports. (d) Medicines consumed while admitted in a hospital/ prescribed by a doctor. (e) Payment made to the healthcare provider by an individual directly or through Health Insurance Company.	Suggesting addition under DHD	may taken for discussion
		Para 3(1)(k) 'Personally Identifiable Information'	It is recommended that <b>instead of 'Personally Identifiable Information', 'Protected Health Information' may be used</b> , as it is more relevant in the present case. And following details may be included for <b>'Personally Identifiable Information' or 'Protected Health Information' in Schedule I</b> : (I) Name. (II) Geographical identifiers smaller than a state i. e. District and below. (III) Dates (other than year) directly related to an individual. (IV) Phone/ FAX Numbers. (V) Email addresses. (VI) Medical record numbers. (VII) Health insurance beneficiary numbers. (VIII) Bank Account numbers/Debit/Credit Card details. (IX) License numbers. (X) Vehicle identifiers i.e. RC numbers. (XI) Web Uniform Resource Locators (URLs) and Internet Protocol (IP) address numbers. (XII) Biometric identifiers, including finger, retinal and voice prints. (XIII) Full face photographic images and any comparable images. (XIV) Any government number, including Aadhar, Voter's Identity, Permanent Account Number ('PAN'), Passport, Ration Card, Below Poverty Line ('BPL'). (XV) Any other unique identifying number.	recommended that instead of 'Personally Identifiable Information', 'Protected Health Information' may be used and also suggesting addition under schedule I	may taken for discussion
		Para 3(1)(n): 'Data Security'	<b>Data related to Protected Health Information (PHI) needs to be secured and not only the Digital Health Data which is subset of the PHI.</b>	Recommendation: Paragraph may be amended as below 'Data Security' refers directly to "Protected Health Information (PHI)", and specifically to the means used to protect the privacy of health information contained in digital health data that supports professionals in holding that information in confidence.	may taken for discussion
		Para 3(1)(o): 'Sensitive Health Related Information'	This is little confusing as a term 'Digital Health Data' has also been mentioned at Section 3(1)(c). All data related to health should be considered as sensitive, however this paragraph is giving an impression as if only some data related health is sensitive and not the complete health data .	Recommendation: <b>Paragraph 3(1)(o) should be deleted.</b>	
		Section 28(1): The rights of the owner of digital health data	<i>The owner of the health data has the right to privacy and a Clinical Establishment has to implement it by ensuring security of this data.</i>	Recommendation: The paragraph may be amended as under: An owner shall have the right to privacy of their digital health data, which may be collected, stored and transmitted in such form and manner as may be prescribed under this Act.	may taken for discussion
		Section 28(2): The rights of the owner of digital health data	This section contradicts the provisions of Section 29 to quite an extent. <b>Electronic Health data is an equivalent of physical records being maintained by clinical establishments and these are very much required so no consent seems to be essential for maintaining legitimate medical records.</b> In fact it is mandatory to maintain medico legal cases. Thus this section should be amended as <b>Clinical Establishment needs to collect and store health data for provision of requisite healthcare services</b> and for future use for benefit of an individual also, so <b>an individual should be given right to give consent to share his/her information along with individually identifiable information or not, like for research.</b>	Express view on contradicts the provisions of Section 29 and right of owner i.r.o of CONSENT	may taken for discussion

## 909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Section 28(3) and Section 28(4): The rights of the owner of digital health data	An individual's right should be limited to give consent to share his/her information along with individually identifiable information or not.	Consent related	may taken for discussion
		Section 41, 42: Obtaining Digital Health Information of another Person & Data Theft	Similar such crimes i.e. data theft and fraudulently obtaining data, are covered under IT Act 2000, so provisions of IT Act 2000 should be made applicable otherwise there can be confusion if punishments are not same in both the Acts.	Data theft	may taken for discussion

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
64			<p>At the outset, please permit me to congratulate you and the Ministry on flagging the importance of a topic, viz. Security and Privacy of Health Data, clearly asserting through this draft that the data owner is unambiguously the patient/citizen/subject whose data it covers, articulating a farsighted vision of Health Information Exchange(s) (atleast for our country; honestly, it has not been fully rolled out in any other country either), clearly positioning the federated model for health and healthcare data (through the hierarchy of centre, state and facilities/clinical establishments) and proposing the Promoter-Regulator 'NeHA' (there seems to be a terminological inconsistency here by referring to Digital Health at the title and earlier sections and suddenly shifting the gear at a later section to e-Health) concept in elaborate details listing it's functions, powers, composition etc. So far so good.</p> <p>Here is the flip side, may be largely caused by elapsed time. Technology has moved on and 'Digital' is all over the place, in the lives of everybody 24x7 ! Smartphones, Cloud, Social networks, Big Data Analytics and AI are changing everything we all do and it is all double disruptive !! Health cannot be left in piece. FitBit and many other devices are measuring our vital parameters every time we make a step. Kindly remember every Android device contains accelerometer, GPS and many other sensors. So, our health data is all over the place and is being tagged by many. So, we need to look at the wider picture to see what is happening, understand how data security and privacy is (or is not) being handled by other stakeholders and then come back to address the data protection and privacy aspects specific to health data and put in place whatever incremental acts, regulations, regulators -promoters and address the institutional issues like functions, powers, members, term, etc.). HIPPA came in another time, another country and another context. <b>This is not the time for us to draft our version of HIPPA. We need to move on and prepare things smarter befitting today's context.</b></p> <p>Let's see what's happening in Data Protection and Privacy nationally and internationally. In India, Supreme court Constitution bench has already pronounced Privacy as a Fundamental Right. So, anything we do in the digital world or 'e-' world must be consistent with that or pass the litmus test of being in conformity with that pronouncement with details thereof.</p> <p>One of the consequence of that is the government forming 'Justice Srikrishna Committee' to address Data Protection and Privacy issues for India and formulate suitable draft law for India (studying global developments and regulations and formulating one that best suits Indian socio-economic, developmental and legal contexts and after consultations with stakeholders) along with other consequential matters like setting up of data controllers etc. (somewhat analogous to what is covered in draft DISHA). The proceedings of that committee set up by MeitY are still on and public sources indicate they are likely to submit their report in the coming months.</p> <p>The core of the above debate is - should India go the GDPR (General Data Protection Regulations) of the European Union (due to come into operation from next month or so) way or any other way (say, USA) (those who want to make it simpler and friendlier to providers of services, public and private). Clearly, <b>devil is in the details and building consensus among stakeholders may take some time and efforts.</b></p> <p>On the top of it, the sand is shifting below our legs all the time. We don't know what it means to have automatic cars, smart homes and voice assistants (in connivance with WiFi bugs and sensors in our TV and other gadgets at home and neighbourhood), smart offices, smart cities (There will be a million CCTVs in our cities before long), sharing data on our daily lives all the time (where should the data be anonymized?!). And we haven't discussed our bank and Fintech issues yet.</p>		
			<p>This draft should await findings of Justice SriKrishna Committee. MoHFW can share their inputs on Data Protection and Privacy aspects from Health sector point of view as the SriKrishna Committee would have sought the comments of many stakeholders. Any one knows wherever there is a discussion on Data Protection and Privacy, Finance and Health always top the list from citizen point of view. While it is true that banks and other entities dealing with finance have been aware of the importance of data protection and privacy (including it's digital cousins or digital masters), health sector has been somewhat slower to take cognizance (especially the 'digital' component of it). Meanwhile, hell has broken out, thanks to Facebook and Cambridge Analytica and has put the spotlight on this topic of privacy and data protection - worldover and in India. So, just have patience to see what comes out on that front and follow up with your share of action. Otherwise, it'll amount to one hand of government not being aware of what the other hand is doing.</p>		
			<p>The draft is too focused on institutional details, at the cost of a build-up on the relevance and importance of the topic, stating key concepts, principles, framework, drivers, linkages to various standards, systems, technologies, vulnerabilities, requirements, controls, testing, audit, certification etc. I do understand that this document has been formulated in the language and format of a draft bill (for instance, like TRAI Act), but that had a context of deregulation and hence the immediate need etc., which are not the case for Digital Health / e-Health / DISHA . Besides, I don't know whether there is a counterpart (Single Point of Contact) regulator for non-Digital Health in the country.</p>		
			<p>The draft, as it has come out now, reads like a justification (a weak one, at that!) to create so many posts! Is that meant to be the thrust? I assume it is not so, but one must be beware of public perceptions !!</p> <p>There are too many typos in the draft.</p> <p>There are places where legal inadequacies appear</p>		

## 909695/2018/E-GOVERNANCE

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
65	Student Initiative for the Promotion of Legal Awareness- SIPLA, NLSIU	Chapter I Section 3(c)	Proviso deals with proxy consent being provided under the Act with regard to usage and transmission of personal health data. As per the S. 30(5) the consent is being contemplated for collection of personal health data into digital health data by clinical establishments and/ or entities for legally, mentally or physically unfit persons for whom the representative or relative shall provide consent.		
		Section 3(m)	Defines relative in a broad manner to include spouse, parents and their brothers and sisters as well as lineal ascendant or descendant of the owner or his/her spouse. This provides a scope of misuse/abuse of the provision by unscrupulous and envious relatives and family connections in disharmonious familial, marriage or inheritance contexts. Hence, it is recommended that the provision of consent by relatives should be restricted to the next of kin i.e. parents and spouse, subject to some exceptions, nominated, selected or affirmed to in some manner by the owner of the health data himself. It can be he is incapable to affirm appoint someone, a provision for independent evaluation of his interests and his bona-fide and beneficial relationship must be conducted by the clinical establishment or entity which obtains this proxy consent. The principle of consent of the individual owner and his rights mentioned in the S. 30 would be vulnerable to prejudice in case the definition of relative is not narrowed and additionally, a pre-emptive and preventive proviso in the S. 3(m) provides for the owner's interest with regard to the relative who obtains the right to give consent.		
		Section 30-i	Exempts the Clinical Establishments owned, controlled or managed by the Armed Forces from the definition of clinical establishment. However, considering the fact that these clinical establishments include highly advanced centers of medical research, treatment and diagnosis for pathological, radiological, chemical investigation which provide healthcare services to certain sections of civilian population, especially in regions of high military concentration like Jammu and Kashmir, Nagaland, Manipur, Assam etc. The utilization/collection of this digital health data for this section of civilians which include the families of the members of the armed forces will be a disproportionate control over their right to informed consent and privacy. Hence, it is recommended that the definition clearly specifies that the exemption is limited to the digital health data of the members of armed forces obtaining certain healthcare and/or medical services but not the civilian population that avails them. The access and control of necessary information in national interest can be otherwise obtained from any clinical establishment, irrespective of being managed by the Armed Forces or not. Hence, this amendment would not impact the reasonable, rational and necessary utilization of personal data of general civilians obtaining services in such establishments but rather protect their health from extraneous control which is intended for legitimate purposes in context of the members of Armed Forces only.		
		S. 30(k)	Defines personally identifiable information to include the information mentioned in the Schedule 1 of the Act. Notwithstanding the reasonable unique identifying features of the other pieces of information in the schedule, the inclusion of entry (x), (xi) and (xiv) namely Financial information, Sexual Orientation and Biometric Information raises concerns about proportionality and data minimization. The sharing of financial information like debit/credit card details provides scope of exploitation by clinical establishments or the other entities involved in collection and transmission process. This is because while the proviso to S. 29(1) mentions that the direct sharing of this information is subject to S. 28 which protects under clause 8(c) the right to prevent sharing of sensitive health related data, the need for this refusal by owner places an undue burden on him to prevent the possible access to potentially prejudicial and sensitive information. Insofar as the delivery of patient centered services and facilitation of coordination of care and information under S.29(1), is concerned, the relevance of information about sexual orientation should be based on the informed decision on the initiative of the owner for his healthcare needs and not merely protected by a subsequent right to prevent such transmission under S. 28. Regarding the position of biometric information under this section, it should also be removed from the schedule as the constitutionality of its utilization for identification purposes in general by administrative and private agencies is sub-judice before the Supreme Court. Hence, it cannot be utilized directly by clinical establishment, pending the supreme court final verdict in this regard.		
		Chapter II Section 5(2)	Chairperson shall have an experience of working as a health administration or preferably health informatics of at least fifteen years. Health Administrator will have the requisite practical experience of the field of health which will help him or her in more holistic understanding of the issues involved than any IT professional or someone from law or public policy.		
		Section 10	provides for appointment of National and State Authorities. It is submitted that a procedure similar to elevation of HC judges to SC can be adopted which will help have more experienced persons for the National Authority.		
		Section 15	It is recommended that the meeting shall be held every four months in order to review or ensure proper functioning of the authority. The draft does not stipulate any time after which such meeting must be held.		
		Chapter III	The investigative powers of authority should be more exhaustive. It should have the power to order clinical establishments, health exchanges and other entities to provide any information it requires for the performance of its tasks. The authority should also carry out investigations in the form of data protection audits. The authority should notify the entities of an alleged infringement or violation of the act or rules/regulations. A provision on this should be included. An investigation without notifying the entities would be arbitrary. Therefore, a provision on providing a notice is necessary. The supervisory authority shall have corrective powers to issue warnings, reprimands and communicate a health data breach to the data subject/entity. Moreover, it should have the power to order the entity to comply with the rules and regulations.		
		Chapter IV Section 28(5)	Provides the owner with the right to have only specific and relevant data collected from him, with it not excessive for the concerned purpose. It must be noted that the enforcement of such a right may prove problematic in light of how the burden is on the data subject to determine whether the data collected is excessive or not, and since the said data subject will usually not have the requisite knowledge to make such an informed decision. Since it is found to be commercially beneficial for medical institutions to collect more patient data, we may find such institutions making undue advantage of the subject's inability to make a reasoned decision.		
		Section 29(1)	Use of the term "generated" in Section 29(1) is problematic since it may indicate that any data "produced" or "developed" by the medical institution about the subject, maybe through the use of some data which the subject has consentually provided, is owned by the medical institution. This would further imply that the medical institution may not need to seek the consent of the subject for use of this "generated" data. It would be in the best interests of the data subject to clarify what is the legal status of ownership of this "generated" data. In our opinion, Section 29(1)(c) is too broad. It would be fairly simple for a medical institution to show the link between collection of personal data and an improvement in the "delivery of patient centered medical care". What is of importance in this regard, however, is the degree of such improvement. We hence seek greater clarity and specify on what an advancement in the delivery of patient centered medical care comes. Since collection under Section 29 is subject to the provision of Section 28, consent is an essential element of such collection. This is rendered problematic in light of Section 29(1)(b) which provides for the purpose of guiding medical decisions at the time and place of treatment. In such contexts, it may be impossible to obtain the explicit consent envisioned under Section 28(2). We seek greater clarity on what the "substitute" to this explicit consent in such situations is. Will consent from a family member/guardian suffice? Will obtaining consent post treatment be representative of the right under Section 28(2), as long as the treatment is done in the best interest of the subject? (The proviso to Clause 29 provides that in case of use of medical data for public health purposes, "only de-identified or anonymized data shall be used". The use of the term "or" is problematic due to the significant difference between de-identified and anonymized data. De-identified means that the personal identifiers in a record have been extracted and that it would be very difficult to re-establish any of the people mentioned in the original record. "Anonymized", on the other hand, means that all of the links between a person and the person's record have been irreversibly broken so that it would be virtually impossible to re-establish any of the people in the original record. This reversibility is of prime importance and could be a determinant factor in the subject deciding whether he wants to consent to the use of his data or not. Hence, we believe there should be greater clarity on whether the data would be de-identified or anonymized.		
		Section 29(3)	speaks of use of data only for the purposes to which the owner has given consent. We believe that in the context of medical institutions, the concept of consent is rendered all the more delicate, in light of emergency situations, for example, where the data subject may not have the ability or frame of mind to provide informed consent. We believe there should be more mechanisms in place to ensure that data subjects, when subject to medical illnesses, do exercise their right to informed consent, in the manner envisioned by the Act.		
		Section 30(2)	We agree with the desirability of having a "template" for notices, as envisioned under Section 30(2). While enforcing this provision however, it must be ensured that the issue of consent fatigue and of bombarding the subject with too much information, as this would result in the subject not reading the same, invalidating the goal of informed consent. The effective enforcement of the same can be ensured through a mechanism of mandating that every medical institution has their notice format and general structure approved by a central regulatory authority or through placing a cap on the length of such notices, for example. Notices have continued to be constructed through the lens of the organization providing the same. The focus now needs to be shifted to a consumer-centric approach, acknowledging that in majority of the cases, data subjects, especially medical patients, who in the moment often have greater concerns, will refrain from reading an excessively long notice, and sign it regardless of its content. Moreover, Section 30(2)(c) is inadequate, it should further cover the authorizations which these recipients have and the uses to which they can put the data. Further, Section 30(2)(c) speaks of conversion to a "digital format", but fails to specify whether this format would imply de-identified or anonymized data.		
		Section 30(5)	introduces the innovative concept of a data subject being allowed to withdraw the proxy consent provided on his behalf. However, this section omits to specify the consequences of such withdrawal. Would the medical institution be obliged to permanently delete all the collected data? What would be the timeframe of the said process? What would be the obligation on third parties that the data has been shared with?		
		Section 31(4)	Section 31(4) mandates that the medium of storage and transmission of data should be owned by the clinical establishment of health information exchange. This may be problematic in light of how numerous hospitals may want to choose to store such information on secure cloud services. Cloud computing enabled management of data allows for much easier and faster transmission of data between two hospitals and hence, may further the provisions of 29(1), for example, The "register" envisioned in Section 33(4) can be extended into that of a consent dashboard, wherein data subjects would be enabled, in real time, to withdraw or amend any consent they have provided, amend the uses to which the data can be put to use etc.		
		Section 34(8)	envisions the scenario in which the data subject dies and provides for access of such data by heirs and representatives. However, this Section makes no reference to the right to be forgotten: that once the data subject dies, he has the right to have all data stored on him permanently deleted. In light of the frequency of data subject deaths in such institutions, it is essential that this Act envision some mechanism to delete the medical data and prescribe a timeframe within which such deletion must be completed.		
		Section 34(9)	in light of the potential degree of anonymity the medical institution has over the content of the notice to be provided, we believe the said notice may often serve its intended role of protecting the data subject. For this reason, we believe the Ministry would be well advised in specifying what exactly needs to be conveyed to the data subject, upon breach. Examples of such provisions include the data subject's rights post breach, compensatory measures, extent of damage and leak etc. Moreover, it may be desirable to have different forms of notices for ordinary and serious breaches.		
		Chapter V Section 37	Rough clause (c) classifies even the substantial storage or transmission of data as a breach. We believe this is a desirable step as it would drive medical institutions to ensure that they do not try to dodge the new technical and security requirements. Moreover, by a reading of Section 37(a), since even mere generation which is not in conformity with the provisions of the Act is a breach, we get the indication that even merely collecting excessive data, not needed for the concerned purpose, may be classified as a breach. We deem this to be a desirable step as it raises the pedestal the data subject is seated on and places privacy and data protection at the heart of the collection of medical data.		
		Section 40(1)	We believe the stringent sanction that has been laid down in Section 40(1), i.e. a minimum of one lakh rupees per day is ideal in the context of personal data protection and in light of contemporary jurisprudence on privacy and data protection. In case of a breach, or even a threat of a breach, time is essential and each day's delay could translate to significant harm to data subjects. By placing the sanction for failing to address data owner grievances at a similar pedestal, the Ministry has once again given the concerns of the data subject more importance at the fore and we support the same.		
		Section 43	prescribes that a Court may take up an offence laid down in this Act only upon the complaint of the Central or State Government or the National or State Electric Health Authority, or by a person affected. This provision is problematic since the victims of data breaches are often unknown, unsuspecting victims, many of whom in a country such as India continue to fail to understand the value and concept of personal data and the legal provisions governing the same.		

909695/2018/E-GOVERNANCE

S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
		Chapter VI Section 45(2) and 45(3)	sets limitation period at two years from knowledge or notification of the breach.It is submitted that in case, a petitioner fails to approach the Authority within this period of 2 years, given that the issue of breach involves Right to Privacy, s/he may approach the High Court directly for which limitation is 3 years.Secondly, the term 'coming to know' in section 45(2) needs to be defined. It is not clear how much knowledge needs to be there to apply this sub-section. So, in absence of any definition, there is scope of arbitrariness in deciding using varied interpretations.		
		Chapter VII S. 52	mentions that the Act would supersede any act with regard to protection of health data record for the time being in force but there is lack of contemplation of its relationship with the principle-based legislative intent and structure of the long-awaited Data Privacy law. A contemplation of harmonization of principles and rules under the Data Privacy law is important		
		Section 58 (5)	provides for comprehensive review of all laws and regulations relating to health by Union as well as State governments within 1 year of coming into force of this Act. Such administrative effort should be expended and expedited before the enactment of this legislation for higher effectiveness and predictability of legislative structure in the country. The consultative process should attempt to reconcile these anomalies before the enactment of this Act.		



Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
66	Bloomberg BNA		<p>Nice speaking to you on the phone just now. As I explained, I am a reporter with Bloomberg BNA, which covers policy and regulatory issues.</p> <p>I want to know from you:</p> <ul style="list-style-type: none"> <li>- what key issues have come up in stakeholder comments sent to the ministry.</li> <li>- whether the ministry is aware about stakeholder concerns about the timing of the DISHA draft, given that an overarching national law on data security and privacy is still in the works.</li> <li>- <b>whether the strict and complete restriction on pharma and insurance companies from accessing digital health data is likely to be retained in the final draft, or if any exceptions might be allowed.</b></li> </ul> <p>I look forward to hearing back from you soon as I am on a deadline.</p>	Just asking status of development of DISHA	No action required

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
67	ConnectedH		<p>Following is a list of points, where further clarification or rethinking on the limits imposed on the roles various players can play:</p> <p><b>Draft explicitly says that Health Information Exchanges can be formed only by central government.</b></p> <p>The first concern is around only allowing the central government to open such exchanges. There are a lot of startups apart from ours, which have the vision to organize and collate the medical information generated in the ecosystem. Many of them have already reached a decent scale, e.g. Practo, and the <b>draft policy doesn't provide any clarification on how would such cases be integrated into the system or handled.</b></p> <p>Also, the rationale for allowing <b>only the government to create such exchanges is a little limiting, limiting in the sense of limiting the role the private sector can play in the initiative.</b> When we have private banks, with tight regulation and oversight of a regulator, why can't we emulate the same in this space?</p> <p><b>The draft policy has no explicit mention/definition of the entities, apart from clinical establishments and health information exchanges, which can collate and store healthcare data. However, there are multiple references to 'other entities' which can collate and store data and will be responsible for safely storing data that lies with them.</b> Here again, the draft policy doesn't provide clarity as to how the players like Practo, or Lab management system providers will be treated as they also have a large amount of healthcare data on their platforms even though they don't fall in any of the two types of players defined in the policy.</p> <p><b>Clause 29, subclause 5, mentions that "Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government." There is no clear definition of what constitutes commercial here, will the CRM solutions used by different labs, clinics and hospitals also come under commercial purpose?</b></p> <p>Gaining a clarity of above points would go a long way in helping startups like us define the roadmap they should take in light of the government's initiatives.</p>	Expressed concerns that this act will limit the scope for private player	May be taken for discussion

## 909695/2018/E-GOVERNANCE

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
68	Aditya Brila Health insurance	Aditya Brila Health Insurance	<p>This is with reference to the proposed draft on "Digital Information Security in Healthcare, act (DISHA)".</p> <p>At the outset our sincere apologies for delay in sending our feedback on the draft Act, but considering far reaching implications we humbly request you to consider our feedback while finalizing the Act.</p> <p>As a Health Insurance Company we welcome the move of the Ministry in creating a strong framework for handling sensitive personal and health data of people. We are thankful to the Ministry in giving us an opportunity to express our views and suggestion on the draft of the Act proposed.</p> <p>In the attached file we are pleased to submit our views/comments on the given exposure draft which will enable Health Insurance companies in discharging its obligations to its customers while ensuring due care in providing necessary controls and security on collecting, using, maintaining and sharing of the personally identifiable information and Digital Health Data.</p> <p>Given an opportunity we will be happy to participate in the discussion and exercise of finalization of the Act.</p>		

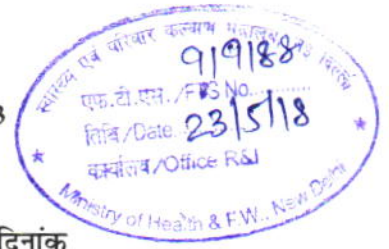
## 909695/2018/E-GOVERNANCE

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
69	Internet and Mobile Association of India-IAMAI	Internet and Mobile Association of India-IAMAI	<p>This is in response to the draft consultation paper of Digital Information Security in Healthcare, Act (DISHA), calling for public comments. The Internet &amp; Mobile Association of India (IAMAI) is happy to submit inputs on the draft paper, by incorporating industry views on the same.</p> <p><b>About IAMAI:</b></p> <p>The Internet and Mobile Association of India [IAMAI] is a young and vibrant association with ambitions of representing the entire gamut of digital businesses in India. It was established in 2004 by the leading online publishers, but in the last 13 years has come to effectively address the challenges facing the digital and online industry including online publishing, mobile advertising, online advertising, e-commerce, mobile content and services, mobile &amp; digital payments, and emerging sectors such as fin-tech, edu-tech and health-tech, among others. Thirteen years after its establishment, the association is still the only professional industry body representing the digital and mobile content industry in India. The association is registered under the Societies Act and is a recognized charity in Maharashtra. With a membership of over 300 Indian and overseas companies, and with offices in Delhi, Mumbai, Bengaluru and Kolkata, the association is well placed to work towards charting a growth path for the digital industry in India.</p> <p>We do hope our submission is given due consideration. On behalf of the membership, we are happy to provide further inputs and/or be involved in any further consultation on the matter.</p>		

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
70	Personal Connected Health Alliance- PCHA		Warm Greetings from Personal Connected Health Alliance (PCHA) ! Please find our comments for the draft of Digital Information Security in Healthcare Act (DISHA) for your kind perusal.		

Comments received on draft Act placed in Public domain "DISHA"					
S.No	Institution / Organisation	Draft Act Clause No	Comment	Finding	Remark
71	28.04.18	Bureau of Indian Standards	<p>This has reference to the the notice dated 21st March, 2018 issued by eHealth section of Ministry of Health &amp; Family Welfare, Govt. of India through which the the draft of "Digital Information Security in Healthcare Act (DISHA)" was placed in public domain for comments.</p> <p>The comments received from members of MHD 17 on the draft are attached and may kindly be considered for incorporation/modification in the draft act. The comments have been duly approved by MHD 17 Chairman, Dr. Ashok Kumar.</p> <p>It may be noted that MHD 17, Health Informatics Sectional Committee is one of the 19 sectional committees under Medical Equipment and Hospital Planning Dept. (MHD) of Bureau of Indian Standards, New Delhi and looks after national standardization work in the area of Health Informatics.</p> <p>The delay in submission of the comments is deeply regretted.</p>		

भारत सरकार  
Government of India  
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय  
Ministry of Electronics & Information Technology  
इलेक्ट्रॉनिक्स निकेतन, 6, सी जी ओ कॉम्प्लेक्स, नई दिल्ली-110003  
Electronics Niketan, 6, C G O Complex, New Delhi-110003  
Website: www.meity.gov.in



संख्या

No.....

दिनांक

Date.....

13(4)/2018-ITEA

17<sup>th</sup> May, 2017

## OFFICE MEMORANDUM

**Subject: Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)" regarding.**

This is with reference to the communication D.O. No. Z-18015/23/2017-eGov dated 21<sup>st</sup> December, 2017 received from Ministry of Health & Family Welfare on the subject cited above.

2. The Draft Act has been examined in Ministry of Electronics and Information Technology (MeitY) and MeitY's comments on the said Draft Act are enclosed.

3. This is issued with the approval of Secretary, MeitY.

Encl: As above.

*Mang*  
(M.K. Jain)

Director

Tele: 011-24301780

*ppst JS (e-Gov)*

*JS - o/T  
Dir(e-gov)*

To:

Shri Lav Agarwal  
Joint Secretary  
Ministry of Health & Family Welfare  
Nirman Bhavan,  
New Delhi-110011



Sl. No.	Clause in DISHA	Comments
1.	<p><b>Definition of Digital Health Data</b> set out in Clause 3(1)(e) means an electronic record of <u>health related information about an individual</u> shall include: (i) Information concerning the physical or mental health of the individual; (ii) Information concerning any health service provided to the individual; (iii) Information concerning the donation by the individual of any body part or any bodily substance; (iv) Information derived from the testing or examination of a body part or bodily substance of the individual; (v) Information that is collected in the course of providing health services to the individual; or (vi) Information relating to details of the clinical establishment accessed by the individual.</p>	<p>The definition of digital health data may be revised to suggest that it is information that could be <u>used to identify an individual</u> instead of stipulating that it includes information “about the individual” or “pertaining to the individual”. In this regard, please note that most data protection legislations follow this approach. For instance, the EU GDPR protects personal data that can be used to identify an individual. Similarly, Health Insurance Portability and Accountability Act, 2006 (HIPAA) protects “personally identifiable information”.</p>
2.	<p><b>3(1)(c) Consent</b> means express informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data. Provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act.</p> <p><i>See also:</i></p> <p><b>Clause 28(2):</b> An owner shall have the right to give or refuse consent for the generation and collection of digital health data by clinical establishments and entities, subject to the exceptions provided in Section 29 of this Act.</p> <p><b>Clause 28(3):</b> An owner shall have the right to give, refuse or withdraw consent for the storage and transmission of digital health data.</p> <p><b>Clause 28(4):</b> An owner shall have the right to refuse consent to the access or disclosure of his or her digital health data, and if refused it shall not be disclosed, subject to the exceptions provided in Section 33 of the Act.</p>	<p>The definition of consent should also include that it is “freely given” and “specific” to the purpose of processing. This means that the individual should not be denied any health service if she refuses to give consent. Further, at the time of seeking consent, the purposes for which the digital health data may be used must be specified to the individual. Please note that it is important that no individual is denied health services upon the withdrawal of consent at a later date.</p>



3.	<p><b>Proxy Consent</b></p> <p><b>Clause 30(5):</b> Without prejudice to the above subsection (2), when an individual is incapacitated or incompetent to provide consent, either due to physical or mental incapacity, the clinical establishment may collect health data by obtaining proxy consent from a nominated representative, relative, care giver or such other person, as may be prescribed under this Act, and who has the legal capacity to consent. Provided that where the individual has regained his or her capacity to give or refuse consent for the collection of his or her health data by the clinical establishment, he or she shall have the option to seek withdrawal of proxy consent and obtaining his or her own consent for collection of such health data, in such form and manner as may be prescribed by the National Electronic Health Authority of India.</p> <p><b>Clause 30(6):</b> Where a person is a minor and it is in the best interest of the minor, proxy consent can be obtained by the minor's legal guardian, or representative. Provided that upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the further collection, storage, transmission of his/her digital health data.</p>	<p>This Bill does not define proxy consent. For instance, HIPAA provides that a "legal representative" must be nominated and can act on behalf of the individual and provide consent or make decisions for the individual where she is not in a position to do the same.</p>
4.	<p><b>Notice</b></p> <p><b>Clause 28(8)(c):</b> The owner of the digital health data shall have the right to be notified every time their digital health data is accessed by any clinical establishment within the meaning of Section 34 of the Act.</p> <p><b>Clause 30(2):</b> A clinical establishment may, by consent from the owner, recorded in the form and manner as may be prescribed under this Act, lawfully collect the required health data, after informing the owner of the following: (a) The rights of the owner as laid down in this Act, including the right to refusal to give consent to the generation and collection of such data; (b) The purpose of collection of such health data; (c) The identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format; (d) The identity of the recipients who may have access to such digital health data on a need to know basis</p>	<p>In addition to what is already stipulated under the relevant clauses, the notice form could also consider including the entity that may be approached for grievance redressal and the procedure for grievance redressal in case of a data breach or any other dispute.</p>
5.	<p><b>Rights of the Data Owner</b></p> <p><b>Clause 28(6):</b> An owner of the digital health data shall have the right to know the clinical</p>	<p>These provisions appear to be similar to the right to seek confirmation; the right to seek access; and the right to seek rectification, as set out under the</p>

	<p>establishments or entities, which may have access to the digital health data, and the recipients to whom the data is disclosed.</p> <p><b>Clause 34(5):</b> The owner of the digital health data shall have a right to access his or her data in such form and manner, as may be specified by the National Electronic Health Authority of India</p> <p><b>Clause 36:</b> An owner of the digital health data shall seek for rectifying the incorrect digital health data stored in any clinical establishment or health information exchange, as the case may be, by making an application in such form and manner as may be prescribed under this Act. (2) On receipt of such application under sub section (1), the clinical establishment or health information exchange shall rectify such digital health data immediately or within three working days from the date of receipt of such application and the same shall be intimated to the owner in writing.</p>	<p>EU GDPR.</p> <p>However, this Bill does not envisage other Individual Participation Rights such as the right to erasure- whereby the data owner can request the data controller to erase or delete her digital health data once the purpose for which it was collected is satisfied; and the right to restrict to processing- in situations where the accuracy of the health data may be in question, or where the processing is unlawful.</p>
6.	<p><b>Storage of Digital Health Data</b></p> <p><b>Clause 32</b></p> <p>(1) No digital health data shall be stored by any clinical establishment or entity or health information exchange in any manner, except in accordance with the provisions of this Act.</p> <p>(2) The clinical establishment or health information exchange, as the case may be, shall hold all digital health data, on behalf of National Electronic Health Authority; and such data be used for such purposes as stated in Section 29, without compromising the privacy or confidentiality of the owner, and security of such data.</p> <p>(3) The digital health data vested with the National Electronic Health Authority as per sub-section 2 above, shall be stored and may be transmitted or used in such form and manner as may be prescribed by the National Electronic Health Authority.</p>	<p>The Bill may also include a provision that specifies that digital health data may be stored only for as long as it may be reasonably necessary to satisfy the purpose for which it was collected.</p>
7.	<p><b>Data Pertaining to Deceased Persons</b></p> <p><b>Clause 34 (8):</b> In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Electronic Health Authority of India. Provided that no access shall be given to legal heirs or legal representatives if it was expressly barred by the owner. Provided further that in case of death of the owner, the National</p>	<p>This Bill contains a unique provision whereby it seeks to protect the digital health data of a deceased individual as well. The EU GDPR, for instance does not extend its protection to the personal data pertaining to a deceased individual. However, the Privacy Rule under the HIPAA grants the power to the legal representative of the individual to act on her behalf in case of death.</p>

	Electronic Health Authority, shall use the digital health data only in anonymised form.	
8.	<p><b>Digital Health Information Exchanges</b></p> <p><b>Clause 3(h):</b> 'Health Information Exchange' means a health information exchange as established under this Act.</p> <p><b>Clause 19:</b> The Central Government shall, by notification, establish as many Health Information Exchanges, as considered necessary, for the purposes for this Act.</p> <p><b>Clause 20:</b> All Health Information Exchanges shall conduct and carry out their affairs strictly as per the norms, standards or protocols specified by the National Electronic Health Authority, or as per Rules prescribed by the Central Government.</p>	<p>Please note that the definition of a "health information exchange" is not sufficiently precise under the Bill. From the Bill, it is unclear what the mandate/scope of function of a Health Information Exchange will be. Considering that a Health Information Exchange will be responsible for the storage and onward transmission of sensitive digital health data, its exact role and function must be described more clearly within the Bill. Additionally, the Bill must clearly contemplate any such Health Information Exchange and its functions/role must be in accordance with data protection principles set out in the Bill, as may be applicable.</p>
9.	<p><b>Data Breaches and Serious Data Breaches</b></p> <p><b>Clause 37-</b> If any person generates, collects, stores, transmits or discloses digital health data in contravention of the Bill, or if any person damages, tampers with or destroys the data, or if the data is not secured in the required manner, then this would amount to breach.</p> <p><b>Clause 38-</b> A serious data breach would include the intentional, dishonest or fraudulent commission of a breach; if the breach occurs to non-anonymised data; or use of digital health data for commercial purposes.</p>	<p>While the Bill sets out the scope of what amounts to a data breach and a serious data breach, and the respective punishments, it does not specify that the data controller (in this case the clinical establishments or the digital Health Information Exchanges) should notify the data owner/individual about the breach without undue delay (the EU GDPR suggests that data breach notification should be carried out within 72 hours of the data controller becoming aware of it). Notification of a data breach should ideally mention the type of data breach, the estimated date of the breach, a brief description of the breach. The notification should also inform the individual of her rights with respect to the breach and whom to contact in order to address grievances.</p>



I/3161141/2018



प्रीति सूदन

सचिव

PREETI SUDAN  
Secretary

भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण विभाग  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय

Government of India  
Department of Health and Family Welfare  
Ministry of Health & Family Welfare

DO No. Z-18015/23/2017-eGov

Dated : 4<sup>th</sup> June, 2018

Dear

As you may be aware that the Ministry of Health and Family Welfare is in process of drafting legislation as **"Digital Information Security in Healthcare, Act (DISHA)"** to regulate, develop standards and strategize & deploy digital health across the continuum of care.

2. The draft DISHA legislation was prepared in consultation with National Law School, Bangalore and NHSRC involving subject experts. With approval of Hon'ble HFM, the draft act was put in public domain at ministry's website on 21.03.2018 for a period of one month for seeking general public comments/ views. This Ministry has also sent the draft act to MeitY vide D.O. letter dated 21st December, 2017 and vide subsequent reminder letter dated 16th January, 2018 requesting their comments / suggestions on the draft act.

3. The **'Substantive Part' of DISHA** act broadly covers the following:

- Confidentiality, privacy, ownership of health data
- Issue of standardization, storage, transmission of data & Health Information Exchange
- Establishment of Regulatory Bodies as National eHealth Authority (NeHA) at national level and State eHealth Authority (SeHA) at State level its roles & power
- Nature of punishment (civil or criminal) etc., for data breach
- Setting up of Adjudicating Authority & Appellate Tribunal

4. Recently, it is noticed that MeitY has also drafted "White paper on Data protection framework in India". This ministry has examined this framework thoroughly to find out whether an independent Act for Health Department is required or it shall be subsumed within the Act being prepared by the MeitY. It is observed that White paper on Data Protection in India developed by MeitY has broadly covered all aspect of the Data Privacy, security and protection and in principle the need for having separate Data protection act for Health sector may not arise.

Contd....2



I/3161141/2018

: 2 :

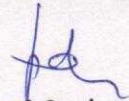
5. Further, this ministry emphases on building interoperability amongst various Health IT Systems to achieve a uniform standard-based system for creation and maintenance of Electronic Health Records (EHRs) of citizens. However to fulfill this, alignment of DISHA and proposed Data Protection framework developed by MeitY is essential and must be ensured.

5. In view of above, you are requested to examine the issue and consider advise whether Ministry of Health need to come up with a separate Act on digital health or else Meity preferably shall come up with a comprehensive Data Protection framework offering domain specific flexibility (such as Health) to define their own standards in proposed framework to avoid multiple data protection legislation.

Early advise is solicited on the issue.



Yours sincerely,



(Preeti Sudan)

Shri Ajay Sawhney,  
Secretary,  
Ministry of Electronics & IT  
Electronics Niketan,  
Lodhi Road, New Delhi-110 003





सत्यमेव जयते

अजय साहनी, आई.ए.एस.  
AJAY SAWHNEY, I.A.S.

By Hand  
Through: D.R.

सचिव

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय  
भारत सरकार

Secretary

Ministry of Electronics &  
Information Technology (MeitY)  
Government of India

D.O. No.:24(3)/2018-CLES  
Dated : 16.07.2018

Dear Preeti,

Thank you for your D.O. letter No. Z-18015/23/2017-eGov dated 4<sup>th</sup> June 2018 regarding Digital Information Security in Healthcare Act (DISHA) which the Ministry of Health and Family Welfare (MoHFW) is in process of drafting that aims to regulate, develop standards and strategize & deploy digital health care across the continuum of care.

2. As mentioned in your letter, with the objective to ensure growth of the digital economy while keeping personal data of citizens secure and protected. A Committee of Experts on Data Protection on 31<sup>st</sup> July 2017, has been constituted vide O.M. No.3(6)/2017-CLES, under the Chairmanship of Justice B.N. Srikrishna, Former Judge, Supreme Court of India. The Committee comprises of members from Government, Academia and Industry, with the aim of studying and identifying key data protection issues and recommending methods for addressing them.

3. The Committee released a White Paper on 27<sup>th</sup> November 2017 to solicit public comments on what shape a data protection law could take. The White Paper outlines key data protection issues and international best practices. We have received responses on the white paper and the Committee is presently at an advanced stage of finalization of its report. The Committee has been requested to submit a report on 'Data Protection Framework' as expeditiously as possible.

4. With reference to concerns regarding overlap between DISHA and the proposed framework, I would like to inform that draft Data Protection Framework includes a clear role for sectoral regulators who will be involved in sector specific guidelines and codes of practice.

With highest regards,

Yours sincerely,

*[Signature]*  
(Ajay Sawhney)

Smt. Preeti Sudan

Secretary

Department of Health &amp; Family Welfare

Ministry of Health &amp; Family Welfare

Nirman Bhawan

New Delhi - 110 011.

Joint Secretary (IA)  
Joint Secretary (IA)

I/3183856/2018

**D.O. No. Z-18015/23/2017-eGov****Dated: 15<sup>th</sup> March, 2018**

Subject: Seeking comments/ suggestion on the draft of "Digital Information Security in Healthcare, Act (DISHA)" -reg.

Dear \_\_\_\_\_,

This is regarding the Digital Information Security in Healthcare (DISHA), Act for setting up of "National Electronic Health Authority of India (NeHA)".

I would like to inform you that the National Health Policy 2017 has delineated specific goals with respect to development of e-health ecosystem in country, some of these includes establishment of national e-health architecture, establishment of health information exchanges and creation of a national authority to regulate, develop and deploy digital health across the continuum of care including issues of privacy, security and digital health data standardization.

Health data is globally accepted to be a 'sensitive data' which deserves to be protected more than other forms of 'personal data'. As of now there is lack of a dedicated and comprehensive legislation/regulation catering to the privacy, security and confidentiality of digital health data/information. The need for statute specifically covering data privacy & security aspects in a comprehensive manner is imperative in the context of promotion & adoption of e-Health on a large scale throughout the country.

In order to address these needs MoHFW has developed draft Digital Information Security in Healthcare (DISHA), Act, after series of consultation and deliberations with various stakeholders.

Salient features of draft act include:

- i . Expressing the 'ownership' of 'digital health data' (with the person/patient to whom the digital health data belongs to

I/3183856/2018

- ii. Establishing a National e-Health Authority and state authorities as a regulatory body for health data standardization in collection, storage, exchange etc.
- iii. Providing for establishment of Digital Health Information Exchanges; and
- iv. Framework to provide for civil and criminal remedies for data breach.

The current draft act (DISHA) has been developed keeping both global best practices and local requirements in mind. We would now like to submit this act for seeking your comments and suggestion on the draft act before putting this up in public domain for feedback.

With Regards

**Lav Agarwal**  
**Joint Secretary**

**To,**

- 1. Principal Secretary (Health) of all States/UTs**
- 2. All JSs, MoHFW**





सत्यमेव जयते

**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195  
T/Fax : 011-23061842  
E-mail. : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011

Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No.Z-18015/23/2017-eGov  
Dated the: 16<sup>th</sup> October, 2018

Dear Sir,

Thank you for your D.O. letter number 24(3)/2018-CLES dated 16.07.2018 apprising that MeitY is drafting a Data Protection Framework which includes a clear role for sectoral regulators who will be involved in sector specific guidelines and codes of practice.

2. It is submitted that the report of the committee under the chairmanship of Justice B. N. Srikrishna, Former Judge Supreme Court of India has been submitted to MeitY. It is, therefore, requested to kindly outline the clear role of Ministry of Health and Family Welfare in respect of Data Protection Framework and further directions, if any, on the draft of Digital Information Security in Healthcare Sector (DISHA) as proposed may be given.

With sincere regards,

Yours sincerely,

(Lav Agarwal)

**Shri Ajay Sawhney**  
Secretary,  
Ministry of Electronic and Information Technology  
Electronics Niketan, 6 CGO Complex  
New Delhi- 110003

I/3192532/2018

D.O. No. Z-18015/23/2017-eGov

Dated October, 2018

Sir,

We are in receipt of your D.O. letter number 24(3)/2018-CLES dated 16.07.2018 apprising that MeitY is drafting a Data Protection Framework which includes a clear role for sectoral regulators who will be involved in sector specific guidelines and codes of practice.

2. It is submitted that the report of the committee under the chairmanship of Justice B. N. Srikrishna, Former Judge Supreme Court of India has been submitted to MeitY. It is, therefore, requested to kindly outline the clear role of Ministry of Health and Family Welfare in respect of Data Protection Framework and further directions, if any, on the draft of Digital Information Security in Healthcare Act (DISHA) as proposed may be given.

With regards

Yours Sincerely

(Lav Agarwal)

To

Shri Ajay Sawhney  
Secretary  
Ministry of Electronic and Information Technology  
Electronics Niketan, 6 CGO Complex  
New Delhi- 110003



**LAV AGARWAL, IAS**  
Joint Secretary

Tel. : 011-23061195

T/Fax : 011-23061842

E-mail. : alav@ias.nic.in



भारत सरकार  
स्वास्थ्य एवं परिवार कल्याण मंत्रालय  
निर्माण भवन, नई दिल्ली - 110011

Government of India  
Ministry of Health & Family Welfare  
Nirman Bhavan, New Delhi - 110011

D.O. No.Z-18015/23/2017-eGov

Dated the: 16<sup>th</sup> October, 2018

Dear Sir,

Thank you for your D.O. letter number 24(3)/2018-CLES dated 16.07.2018 apprising that MeitY is drafting a Data Protection Framework which includes a clear role for sectoral regulators who will be involved in sector specific guidelines and codes of practice.

2. It is submitted that the report of the committee under the chairmanship of Justice B. N. Srikrishna, Former Judge Supreme Court of India has been submitted to MeitY. It is, therefore, requested to kindly outline the clear role of Ministry of Health and Family Welfare in respect of Data Protection Framework and further directions, if any, on the draft of Digital Information Security in Healthcare Sector (DISHA) as proposed may be given.

With sincere regards,

Yours sincerely,

  
(Lav Agarwal)

**Shri Ajay Sawhney**  
Secretary,  
Ministry of Electronic and Information Technology  
Electronics Niketan, 6 CGO Complex  
New Delhi- 110003